BLIND DEMODULATION OF PASS BAND OFDMA SIGNALS AND JAMMING BATTLE DAMAGE ASSESSMENT UTILIZING LINK ADAPTATION

THESIS

Nicholas A. Rutherford, Flight Lieutenant, RAAF

AFIT-ENG-14-M-65

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

AFIT-ENG-14-M-65

BLIND DEMODULATION OF PASS BAND OFDMA SIGNALS AND JAMMING BATTLE DAMAGE ASSESSMENT UTILIZING LINK ADAPTATION

THESIS

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
in Partial Fulfillment of the Requirements for the
Degree of Master of Science in Electrical Engineering

Nicholas A. Rutherford, B.S.E.E.
Flight Lieutenant, RAAF

March 2014

AFIT-ENG-14-M-65

BLIND DEMODULATION OF PASS BAND OFDMA SIGNALS AND

JAMMING BATTLE DAMAGE ASSESSMENT UTILIZING LINK ADAPTATION

Nicholas A. Rutherford, B.S.E.E.
Flight Lieutenant, RAAF

Approved:

//signed// 13 Mar 2014

Dr. Richard K. Martin, PhD (Chairman) Date

//signed// 13 Mar 2014

Dr. Robert F. Mills, PhD (Member) Date

//signed// 13 Mar 2014

Dr. Micheal A. Temple, PhD (Member) Date

AFIT-ENG-14-M-65

Abstract

This research focuses on blind demodulation of a pass band Orthogonal Frequency Division Multiple Access (OFDMA) signal so that jamming effectiveness can be assessed; referred to in this research as Battle Damage Assessment (BDA). The research extends, modifies and collates work within literature to perform a new method of blindly demodulating of a passband OFDMA signal, which exhibits properties of the 802.16 Wireless Metropolitan Area Network (MAN) OFDMA standard, and presents a novel method for performing BDA via observation of Sub Carrier (SC) Link Adaptation (LA).

Blind demodulation is achieved by estimating the carrier frequency, sampling rate, pulse shaping filter roll off factor, synchronization parameters and Carrier Frequency Offset (CFO). The blind demodulator's performance in AWGN and a perfect channel is evaluated where it improves using a greater number OFDMA Downlink (DL) symbols and increased Cyclic Prefix (CP) length. Performance in a channel with a single multi-path interferer is also evaluated where the blind demodulator's performance is degraded.

BDA is achieved via observing SC LA modulation behavior of the blindly demodulated signal between successive OFDMA DL sub frames in two scenarios. The first is where modulation signaling can be used to observe change of SC modulation. The second assumes modulation signaling is not available and the SC's modulation must be classified. Classification of SC modulation is performed using sixth-order cumulants where performance increases with the number of OFDMA symbols. The SC modulation classifier is susceptible to the CFO caused by blind demodulation. In a perfect channel it is shown that SC modulation can be classified using a variety of OFDMA DL sub frame lengths in symbols. The SC modulation classifier experienced degraded performance in a multi-path channel and it is recommended that it is extended to perform channel equalization in future work.

Table of Contents

Page

List of Figures

Figure Page

Figure Page

List of Tables

List of Acronyms

Acronym	Definition
OFDMA	Orthogonal Frequency Division Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
LOS	Line of Sight
SC	Sub Carrier
SNR	Signal to Noise Ratio
RF	Radio Frequency
LTE	Long Term Evolution
ISI	Inter Symbol interference
FEC	Forward Error Correction
MAC	Medium Access Layer
BDA	Battle Damage Assessment
PHY	Physical Layer
FFT	Fast Fourier Transform
IFFT	Inverse Fast Fourier Transform
CP	Cyclic Prefix
LA	Link Adaptation

Acronym	Definition
DL-PUSC	Down Link - Partial Usage of Sub Carriers
DL-FUSC	Down Link - Full Usage of Sub Carriers
PRBS	Pseudo-Random Binary Sequence
FDD	Frequency Division Duplex
TDD	Time Division Duplex
DL	Downlink
UL	Uplink
TTG	Transmit Transition Gap
RTG	Receive Transition Gap
FCH	Frame Control Header
PN	Pseudo Noise
CFO	Carrier Frequency Offset
IF	Intermediate Frequency
ARQ	Automatic Repeat Request
AWGN	Additive White Gaussian Noise
STO	Sample Time Offset
AMC	Automatic Modulation Classification
BER	Bit Error Rate

Acronym	Definition
BW	Bandwidth
PSD	Power Spectral Density
MSB	Most Significant Bit
LSB	Least Significant Bit
ML	Maximum Likelihood
FIR	Finite Impulse Response
MAN	Metropolitan Area Network

BLIND DEMODULATION OF PASS BAND OFDMA SIGNALS AND
JAMMING BATTLE DAMAGE ASSESSMENT UTILIZING LINK ADAPTATION

I. Introduction

This chapter provides the basis of this research including motivation, background and goals. Assumptions and an outline of the thesis are also detailed.

1.1 Motivation

The United States Military, and its coalition partners, consider the ability to dominate the Radio Frequency (RF) spectrum in the modern battlefield a key objective. An aspect of the control of the RF spectrum is the ability to intercept an adversary's communications for intelligence and combat information, or to deny exchange of information encumbering the adversary's ability to make decisions. A rapidly emerging communication technology used in the modern battlefield, and by the civilian sector, is broadband wireless communications utilizing Orthogonal Frequency Division Multiplexing (OFDM) and its multiplexing scheme OFDMA. OFDM includes applications including but not limited to fixed or last-mile wireless access, back hauling, mobile cellular network, and satellite communications by both civilian and military operators. Further, broadband wireless technologies are rapidly emerging in the Middle East and North Africa as primary communication systems to replace existent wired infrastructure, or provide broadband communications in areas where wired infrastructure does not exist. As many of the countries within these aforementioned regions contain potential security threats, and the extensive employment of OFDM in both military and civilian sectors, it is important to develop techniques and technologies to control OFDM based communication.

1.2 Background

Over the past few years there has been increasing emphasis to extend wired broadband communications services to mobile devices. The technologies which support wired broadband communications, however, can not be extended to wireless broadband communications without significant complexity due to the nature of the wireless transmission channel. Consequently, to achieve broadband wireless communication requires technologies which are adept in the wireless transmission channel and can support high data rates with minimum complexity. OFDM, which has been employed in military since the mid 1960s [3], is a communications technology which has experienced rapid deployment in the civilian sector during the past decade due its performance in wireless transmission channels and the reduced costs of microprocessors. OFDM, and its multiplexing scheme OFDMA, are currently employed in various communication technologies, however, of interest to this research are wireless broadband communications technologies such as Long Term Evolution (LTE) and WiMax [4].

This research is focused on the blind demodulation of pass band wireless broadband OFDMA signals in order provide capability to assess the success of communication jamming referred to as BDA in this work. BDA is important when exploiting an adversary's communications as it provides the ability to assess the effectiveness of a jamming technique. This is important as the success of communications exploitation is typically not directly observable. Feedback provides a means to improve exploitation techniques and provides confidence to a commander that the communications of an adversary are successfully suppressed.

802.16 WirelessMAN-OFDMA is a particular standard that defines a wireless broadband OFDMA implementation and has been selected as the basis of the signal model used for this research. The signal developed in this research employs many properties of the 802.16 WirelessMAN-OFDMA standard, however, it is not a true analogue as the signal is simplified to only exhibit the properties required to complete this research. Other OFDMA standards such as that specifying the DL of LTE could have been adopted, however, the differences in the standards do not impact the conclusions of this research.

1.3 Goals

The expected result of this research is to determine a new method to blindly demodulate a pass band OFDMA signal, akin to that defined in IEEE 802.16 WirelessMAN-OFDMA, by extending, modifying and collating work within literature concerned with OFDM signals and present a novel method for performing BDA, on the demodulated signal, via observing modulation LA. The work is focused on performing blind demodulation and BDA by observing modulation change between successive OFDMA DL sub frames in two scenarios. The first is where a civilian standard is used. In this case once the OFDMA synchronization parameters have been estimated the signaling information, such as the burst profile, can be used to observe LA. The second scenario assumes an OFDMA signal where the signaling information is not known, such as a military communication system, and the modulation on the OFDMA SC must be classified in order to perform BDA. Modulation type in this case is classified utilizing sixth order cumulants. To perform BDA the signal must be blindly demodulated, hence, the research presents methods to determine the OFDMA's synchronization parameters including those required to translate it from pass band to base band. The research presents results from simulations of the proposed blind demodulation and BDA model at different noise levels and number of symbols per DL sub frame. Performance in a perfect channel and single multi-path is evaluated. Although this research is primarily focused on wireless OFDMA signals, the methods applied in this research may be used on wireless OFDM due to shared properties.

1.4 Assumptions

The assumptions made to complete this research are:

- only an OFDMA signal is received in the channel,
- an OFDMA Time Division Duplex (TDD) frame structure is employed,
- the carrier frequency is estimated with a maximum error of half the SC spacing,
- the received signal is oversampled by a minimum of a factor of two,
- there is no Sample Time Offset (STO),
- a square root raised cosine filter is used for pulse shaping,
- SC modulation is constant over a DL sub frame, and
- the OFDMA implementation employs LA.

These assumptions are explored further in Chapter II and III.

1.5 Organization

Chapter II presents an introduction to OFDM and OFDMA and details the signal properties that are employed in this research. Further, the methodologies from literature to perform blind demodulation of OFDM signals are extended, modified and collated for OFDMA signals and a novel approach to perform BDA via observing LA is introduced. To perform LA a method of classifying SC modulation is detailed. Chapter II also introduces work related to this research. Chapter III presents the proposed models of the methods outlined in Chapter II, their implementation in simulation, and individual estimator and classifier performance. Chapter IV details of the overall performance of the proposed models in a perfect and single multi-path channel. Conclusions and possible future work are presented in Chapter V.

II. Background

This chapter provides the background for the topics involved in this research. First, there is an introduction to OFDM and OFDMA modulation, followed by the DL specifications of the IEEE 802.16 WirelessMAN-OFDMA standard pertinent to this thesis. Next, the process to blindly demodulate a pass band OFDMA signal is detailed and the method to perform BDA by observing LA is introduced. Lastly, relevant prior research is discussed.

2.1 Introduction to OFDM and OFDMA

Wireless radio channels are characterized by multi path reception where the signal received contains the direct Line of Sight (LOS) radio wave and reflected radio waves which arrive with different delay times [3]. Delayed signals occur due to reflection from terrain features in the wireless channel. The delayed signals interfere with the direct LOS signal and cause Inter Symbol interference (ISI) degrading mobile wireless communications. To overcome multi path reception complex equalization techniques for single carrier modulation schemes may be used at the receiver, however, for broadband mobile wireless communications there are practical difficulties in operating this equalization at several megabits per second with low cost hardware [3]. OFDM offers an alternative to reduce the influence of the multi path fading environment and ISI with low complexity and ultimately achieve broadband wireless communications.

When establishing broadband wireless networks it is also important to service multiple users simultaneously. OFDMA is the multiplexing scheme for OFDM which allows multiple access by sharing SCs and time slots. OFDMA inherits all of the properties of OFDM and also exhibits new features as multiplexing allows packing many user packets into one DL and Uplink (UL) frame. Consequently, OFDMA becomes very efficient in the sense that overheads caused by inter frame spacing can be minimized [5].

The fundamentals of OFDM and OFDMA and how they are implemented in the IEEE 802.16 WirelessMAN-OFDMA standard are detailed in the following sections. Although not the focus of this research an introduction to OFDM is detailed as OFDMA builds on its properties. This enables the methods devised in this work to be generally transferable to OFDM.

2.1.1 OFDM.

OFDM is a multi carrier transmission scheme where a single high rate data stream R is divided over N_b lower rate SCs to overcome the multi path fading environment [3]. On the N_b lower rate SCs information bits are segmented into symbols. The number of bits per symbol is determined by channel conditions and its control in noise varying channels is a method of LA. The importance of LA to this research will be discussed in Section 2.4. The number of symbol levels M on the N_b SCs is determined by the number of bits per symbol l as

$$M = 2^l. \tag{2.1}$$

Typically in OFDM systems the modulation types BPSK, QPSK, QAM-16 and QAM-64 are employed where l is 1, 2, 4 and 8 respectively. These are the SC modulation types considered in this research.

The created N_b data symbols, known as the frequency domain sequence $X[k]$, are then processed by an N_b length Inverse Fast Fourier Transform (IFFT) operation producing a time sequence $x[n]$ of N_b samples

$$x[n] = \frac{1}{\sqrt{N_b}} \sum_{k=0}^{N_b-1} X[k] e^{j\frac{2\pi kn}{N_b}}, n = 0, 1, 2, ..., N_b - 1. \tag{2.2}$$

The resulting block of time samples is known as a single OFDM symbol, and the process can be repeated to create additional OFDM symbols. The time interval between the

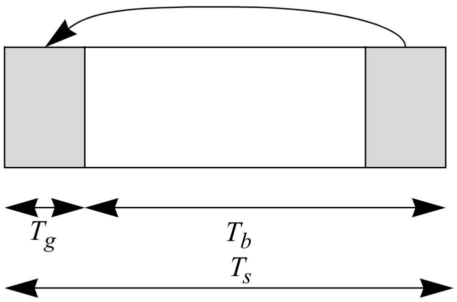


Figure 2.1: OFDM time domain structure from [1].

time samples, T_S, determines the signal Bandwidth (BW) where the N_b SCs are distributed equally. The duration of an OFDM symbol is

$$T_s = T_S(N_b + N_G), \tag{2.3}$$

where N_G represents the CP duration in samples. The CP is a copy of the N_G last samples of the OFDM symbol and is used to collect multi path, while maintaining orthogonality of the tones. The length of the CP varies according to the delay spread of the wireless channel and is typically a ratio of the number of SCs of order $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{16}$, $\frac{1}{32}$. These are the CP orders considered in this research. The CP is removed at the receiver prior to performing the Fast Fourier Transform (FFT) operation to demodulate the transmitted data. The cost of the CP is increased transmission energy and a reduced data rate. Once specified by the base station the CP does not change between frames as it would cause subscribers to resynchronize [1]. The time and frequency domain structure of OFDM are presented in Figure 2.1 and Figure 2.2 respectively.

Unlike the above definition suggests OFDM does not typically modulate information onto all N_b SCs. Instead SCs are modulated as data, pilots for various estimation and synchronization purposes as they are known a priori by the receiver, and null which are used for upper and lower guard bands in an effort to reduce adjacent channel interference

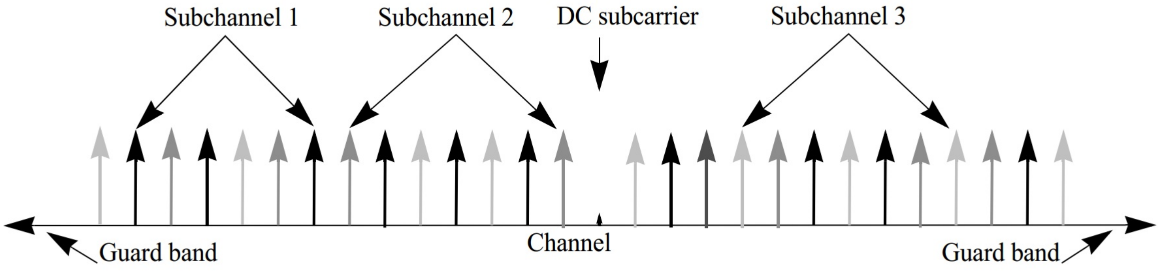


Figure 2.2: OFDM frequency domain structure from [1].

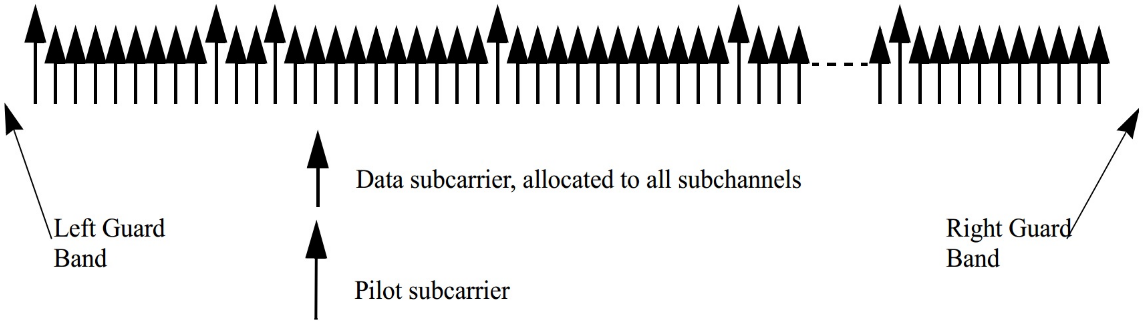


Figure 2.3: OFDM frequency domain structure with various SC types from [1].

or as a DC carrier which is the center SC for a base band signal. Figure 2.3 presents a frequency representation of the OFDM signal with the various SC types.

The number of SCs employed in OFDM is scalable in order to improve data rates. In this process the FFT size increases, where typical FFT sizes are 128, 512, 1028 and 2048. A 128 FFT size is considered in this research to reduce computational complexity and as it is expected to have the worst estimator performance as the number of samples per symbol and CP length, which the blind demodulator process exploits, is smallest. Increasing FFT size typically increases the BW as the frequency spacing between SCs is fixed. The frequency spacing in OFDM is minimized by overlapping the spectrum of individual SCs by exploiting orthogonality of adjacent SCs to avoid interference. Also, as SCs are orthogonal to each other inter-carrier guard bands are not required improving spectral efficiency.

In addition to the use of the CP and guard SCs to reduce interference, OFDM also typically employs error correction coding to correct narrow band interference which affects a small number of SCs. Error correction coding is not considered in this research as the data bits are not considered for blind demodulation or BDA models.

2.1.2 OFDMA.

Physically an OFDMA signal is the same as an OFDM signal, however, the SC modulation is divided in both time and frequency, known as sub channelization, to allow multiple access. Sub channels may consist of adjacent SCs, or SCs pseudo randomly distributed across the frequency spectrum. Sub channels form the resource unit allocation for the base station to assign to multiple users. Sub channelization of a single OFDMA symbol is presented in Figure 2.2 and will be further explored in the following section.

2.2 IEEE 802.16 WirelessMAN-OFDMA Standard - MobileWiMax

In this section the aspects of the IEEE 802.16 WirelessMAN-OFDMA standard, known as MobileWiMax, pertinent to this thesis are discussed. The DL portion of the Medium Access Layer (MAC) and the Physical Layer (PHY) layers of MobileWiMax are introduced only as they are required to complete this research's goal. As other aspects of the signal are ignored, the developed signal is not a true analogue of the standard. Other OFDMA standards such as that specifying the DL of LTE could have been adopted, however, the differences in the standards do not generally impact the conclusions of this research as exploited parameters are shared. The following sub sections detail sub channelization using the carrier permutations schemes and the MobileWiMax frame structure.

Table 2.1: DL-PUSC SC permutation parameters from [1]

FFT Size =	**128**
# of Clusters, N_C	6
# of groups	3
# of sub channels, N_S	3
# Data SC, N_{DSC}	72
# Pilot SC	12
# Right guard carriers	21
# Left guard carriers	22
# SC per cluster	14
Renumbering Sequence, R_S	[2, 3, 1, 5, 0, 4]
Permutation sequence, P	[1]

2.2.1 MobileWiMax PHY SC Permutation Schemes.

MobileWiMax specifies two different SC grouping methods in the DL to realize sub channelization; adjacent and distributed [1]. The adjacent scheme, named band adaptive modulation and coding, operates by grouping a block of contiguous data SCs. Distributed permutation is implemented as Down Link - Full Usage of Sub Carriers (DL-FUSC) and Down Link - Partial Usage of Sub Carriers (DL-PUSC) where sub channels are allocated SCs pseudo randomly which increases frequency diversity. DL-PUSC is the only mandatory permutation scheme and hence is employed in this research. The parameters for the DL-PUSC scheme are defined according to the FFT size. The parameters used within this thesis are concerned with a size 128 FFT and are detailed in Table 2.1. Other FFT sizes used within the standard are 512, 1024, and 2048 where the increase of FFT size scales the permutation parameters.

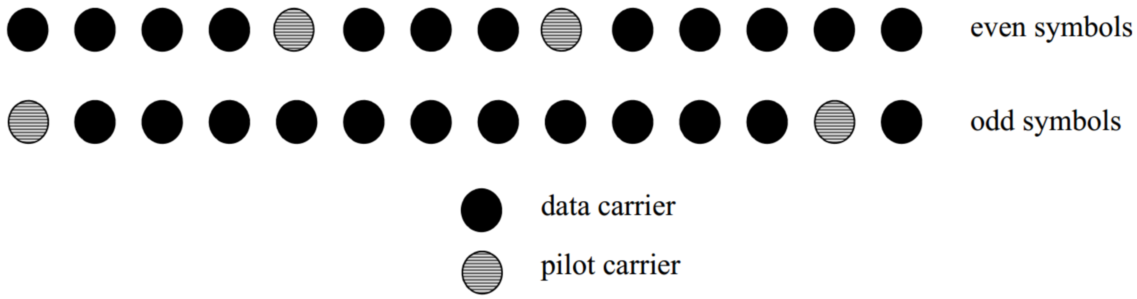


Figure 2.4: OFDMA cluster structure from [1].

The SC allocation in DL-PUSC is performed by firstly dividing the data SCs into the specified number of clusters, N_C, containing 14 adjacent SCs each for all FFT sizes. These clusters are known as the physical clusters, C_P, and their structure is presented in Figure 2.4. Figure 2.4 also shows physical pilot locations which alternate for odd and even symbols where the first OFDMA symbol is even.

Next the physical clusters using the given pseudo random renumbering sequence, R_S, for the FFT size, are renumbered into logical clusters, C_L, as [1]

$$C_L = R_S\left[C_P\right], \tag{2.4}$$

or

$$C_L = R_S\left[(C_P + 13 \times \text{DL\_PermBase}) \bmod N_C\right], \tag{2.5}$$

where the DL_PermBase is an integer ranging between 0 and 31 which is set to the IDCell in the first zone and determined by DL-MAP in other zones. The DL-MAP will be discussed in following sections. A zone refers to a region where the same SC permutation scheme is used. In Mobile WiMax only one zone is required, yet others may be employed, which uses DL-PUSC. Equation (2.4) is used in the first DL zone or when a certain parameter is set in the DL-MAP. Equation (2.5) is used otherwise and is what is employed in this research. After renumbering the logical clusters are divided into groups where cluster size is determined by the FFT size. For a size 128 FFT the logical clusters are divided into 3 groups labeled 0, 2 and 4, where group 0 includes logical clusters 0-1, group 2 includes logical clusters 2-3, and group 4 includes clusters 4-5. Lastly, a sub channel is formed by using two logical clusters from the same group, where for FFT size of 128 there are only 3 possible sub channels corresponding to each group. Lastly, the SCs are allocated to sub channels in each group which is performed separately for each OFDMA symbol utilizing a permutation sequence specific to the FFT size for odd and even groups [1]. The following equation is used to partition SC into sub channels [1]

$$C_{k,s} = N_S \cdot n_k + \{P_S\,[n_k \bmod N_S] + \text{DL\_PermBase}\} \bmod N_S, \tag{2.6}$$

where $C_{k,s}$ is the SC index of the k SC in sub channel s, and s is the index number of a sub channel from the set $[0...N_S - 1]$, P_S is the series obtained by rotating the basic permutation sequence, P, cyclically to the left s times. n_k is defined as [1]

$$n_k = (k + 13s) \bmod N_{SC} \tag{2.7}$$

where N_{SC} is the number of SCs per sub channel.

The pilots in DL-PUSC SC assignment scheme are modulated using a Pseudo-Random Binary Sequence (PRBS). A shift register with 11 stages is shown in Figure 2.5 where the Least Significant Bit (LSB) is the left most bit and the Most Significant Bit (MSB) is the right most bit.

The sequence w_k is generated using the shift register with irreducible polynomial [1]

$$w_k = X^{11} + X^9 + 1, \tag{2.8}$$

where w_k is the used to generate the value of the pilot modulation on SC k. The pilot SCs are modulated according to [1]

$$\text{Re}\{c_k\} = \frac{8}{3}\left(\frac{1}{2} - w_k\right) \cdot p_k, \tag{2.9}$$

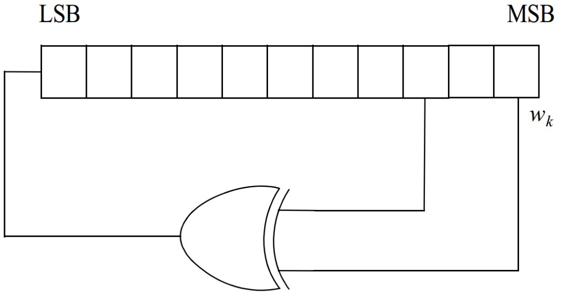


Figure 2.5: PRBS generator used for pilot modulation from [1].

$$\mathrm{Im}\{c_k\} = 0, \tag{2.10}$$

where p_k is the pilot's polarity which is 1 for DL-PUSC and c_k is the modulated value. Note that this modulation represents a scaled BPSK modulation and for DL-PUSC the transmit power of pilot SCs is boosted by 2.5 dB over data SCs.

2.2.2 MobileWiMax Frame Structure.

The two frame structures used in MobileWiMax are Frequency Division Duplex (FDD) and TDD. In FDD the UL and DL sub frames are transmitted simultaneously on different carrier frequencies, while TDD transmits the UL and DL sub frames on the same carrier frequency at different times. Although both frame structures may be used, TDD tends to the preferred method [3] and consequently is the concern of this research. The frame structure of TDD is presented in Figure 2.6.

In Figure 2.6 it can be observed that a TDD frame is composed of an DL and UL sub frame. Each frame in the DL transmission begins with a preamble followed by a DL transmission period, consisting of OFDMA symbols, and an UL transmission period where the ratio of DL to UL sub frame length varies between 3:1 and 1:1 as required. Guard zones, known as a Transmit Transition Gap (TTG) or Receive Transition Gap (RTG), are inserted between the sub frames to separate them allowing the base station and subscribers to transition between receive and transmit modes. Following the preamble each DL and UL sub frame is divided into zones which each may use a different SC permutation scheme. The permutation sequence used within the research is DL-PUSC is illustrated in the figure. This scheme is selected as it is the only mandatory scheme prescribed by the MobileWiMax standard. To allow base station and subscribers to receive a particular zone of information the starting location and the duration of the various zones being used is provided by control messages in the beginning of each DL sub frame.

Other important sections of the frame are the preamble, Frame Control Header (FCH), DL-MAP, UL-MAP, and UL ranging [3]. The preamble is the first OFDMA symbol in the DL sub frame. The preamble is known a priori and used for frequency synchronization, and initial channel and interference estimation. The generation of the preamble is detailed in the following sub section. The FCH follows the preamble and provides information on the frame configuration such as the SCs used, the ranging sub channels, and the properties of the DL-MAP. The DL-MAP and UL-MAP details sub channel allocation and other control information such as the burst profile for each user in the DL and UL sub frames. The UL sub frame contains the UL ranging sub channel which enables closed-loop time, frequency, and power adjustment as well as BW requests [3].

It also can be noted in Figure 2.6 that the OFDMA symbol number increases by 2, this is the minimum allocatable unit of the frame known as slot. The slot definition varies for the SC permutation scheme used where for DL-PUSC it is defined as 24 data SC $\times$ 2 OFDMA symbols.

For this research only the DL sub frame is implemented as we are trying to affect the information transmitted from the base station to the user. Different DL sub frame lengths, in OFDMA symbols, are utilized in this research where lengths are not adopted from a specific standard. Rather, symbol lengths of 25, 75, and 250 symbols are considered to represent possible DL sub frame lengths in practical OFDMA implementations. The DL sub frame is generated with a preamble, as per the following section, and all other sections

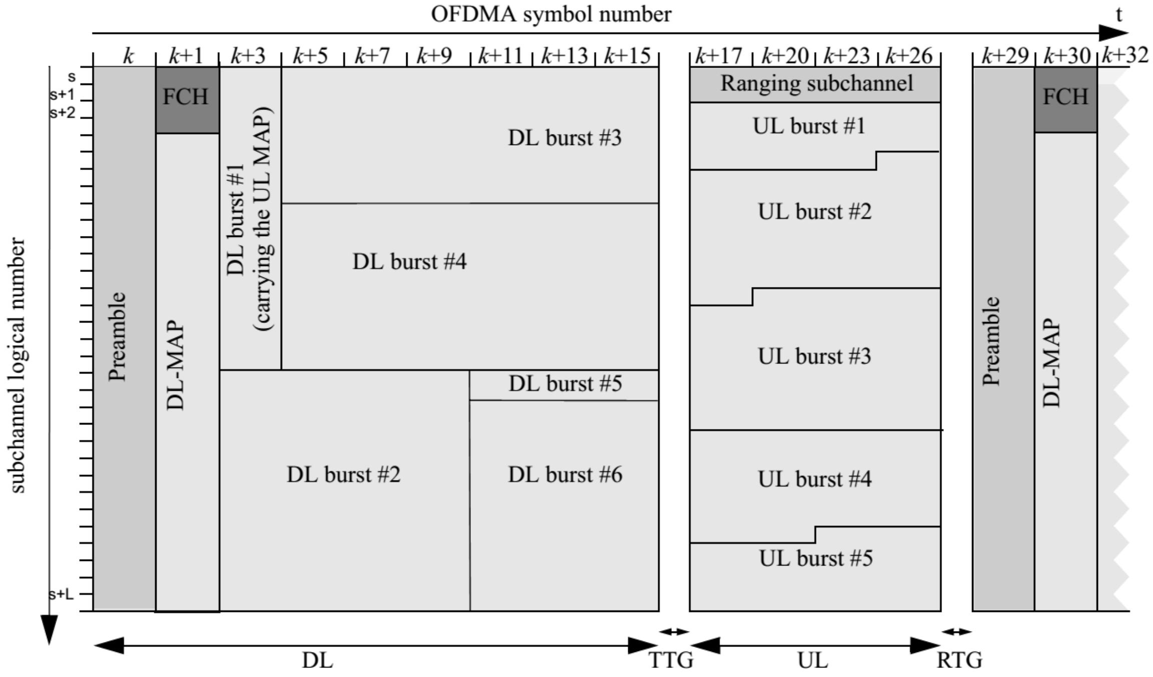


Figure 2.6: TDD frame structure with UL and DL sub frames from [1].

of the sub frame are modulated on SCs with a fixed modulation type. For this work it is assumed the SC modulation type does not change within each DL sub frame, however, may vary between DL sub frames due to LA. Modulation change between sub frames enables BDA via observing LA.

2.2.3 DL Preamble Generation.

The preamble is the first symbol in the DL transmission and the preamble SCs sets are selected according to FFT size. For all FFT sizes the SCs are modulated using a boosted BPSK signal using a Pseudo Noise (PN) code. The preamble carrier sets, C, are defined as [1]

$$C_n = n + 3k, \tag{2.11}$$

where $n = 0, 1, 2$ is segment number and k is a running index which for the size 128 FFT is the integers 0-35. Consequently, each carrier set utilizes a different set of SC. From this definition it can be observed that each segment modulates every third SC.

A predefined PN series is then used to modulate the preamble carrier set. The hexadecimal PN series for the size 128 FFT is defined in Table 2.2. In addition, for the size 128 FFT preamble 10 guard band SCs are employed on each side of the spectrum. The boosted BPSK signal is then modulated onto the carrier set as

$$\mathrm{Re}\{c_k\} = 4\sqrt{2}\left(\frac{1}{2} - w_k\right), \tag{2.12}$$

$$\mathrm{Im}\{c_k\} = 0, \tag{2.13}$$

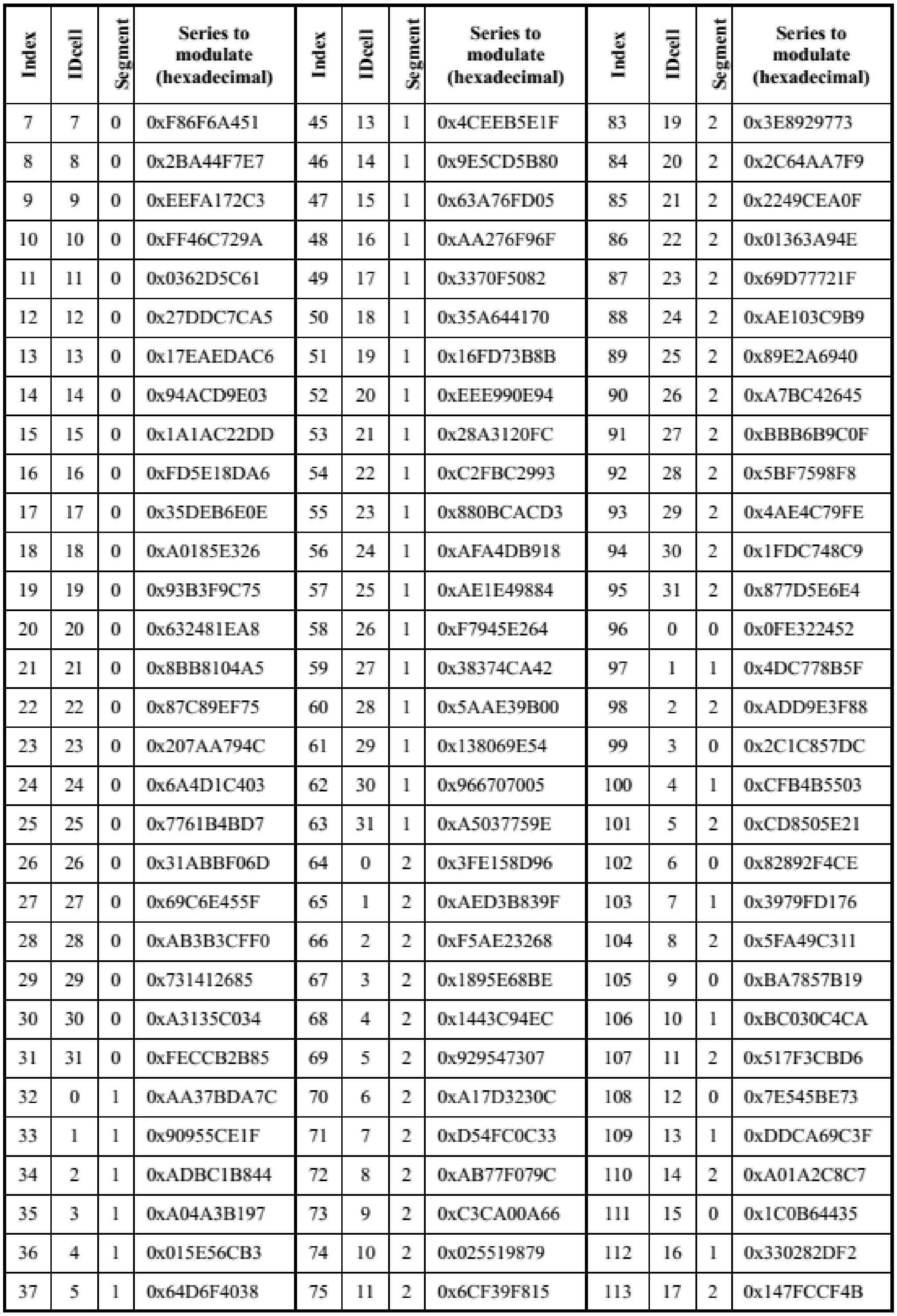
where w_k is the binary PN series and c_k is the value modulated on the k SC in the carrier set.

It can be noted that 114 different series can be modulated for the size 128 FFT. The specific preamble set does not have an impact on this work as the blind demodulator exploits the time domain samples and CP structure properties which does not vary with preamble series. Consequently, the first series is chosen in Table 2.2.

2.2.4 Burst Profiles.

The burst profile is the message which contains information about various parameters of a burst including the modulation type, Forward Error Correction (FEC), preamble type and guard times. The burst profile is a part of both the DL and UL sub frames. The burst profile is important to this research as it provides the means, if available, to perform BDA by observing SC modulation change. The burst profile in the simulations is not generated, rather, it is assumed whether it is available or unavailable in the DL sub frame once the signal is demodulated. The case where it is unavailable is due to deviation from a civilian standard, which may occur in military signals. In this case the SC modulation type is classified and this is detailed in subsequent sections.

Table 2.2: Preamble modulator series according to IDCell and Segment from [1].



Index	IDcell	Segment	Series to modulate (hexadecimal)	Index	IDcell	Segment	Series to modulate (hexadecimal)	Index	IDcell	Segment	Series to modulate (hexadecimal)
7	7	0	0xF86F6A451	45	13	1	0x4CEEB5E1F	83	19	2	0x3E8929773
8	8	0	0x2BA44F7E7	46	14	1	0x9E5CD5B80	84	20	2	0x2C64AA7F9
9	9	0	0xEEFA172C3	47	15	1	0x63A76FD05	85	21	2	0x2249CEA0F
10	10	0	0xFF46C729A	48	16	1	0xAA276F96F	86	22	2	0x01363A94E
11	11	0	0x0362D5C61	49	17	1	0x3370F5082	87	23	2	0x69D77721F
12	12	0	0x27DDC7CA5	50	18	1	0x35A644170	88	24	2	0xAE103C9B9
13	13	0	0x17EAEDAC6	51	19	1	0x16FD73B8B	89	25	2	0x89E2A6940
14	14	0	0x94ACD9E03	52	20	1	0xEEE990E94	90	26	2	0xA7BC42645
15	15	0	0x1A1AC22DD	53	21	1	0x28A3120FC	91	27	2	0xBBB6B9C0F
16	16	0	0xFD5E18DA6	54	22	1	0xC2FBC2993	92	28	2	0x5BF7598F8
17	17	0	0x35DEB6E0E	55	23	1	0x880BCACD3	93	29	2	0x4AE4C79FE
18	18	0	0xA0185E326	56	24	1	0xAFA4DB918	94	30	2	0x1FDC748C9
19	19	0	0x93B3F9C75	57	25	1	0xAE1E49884	95	31	2	0x877D5E6E4
20	20	0	0x632481EA8	58	26	1	0xF7945E264	96	0	0	0x0FE322452
21	21	0	0x8BB8104A5	59	27	1	0x38374CA42	97	1	1	0x4DC778B5F
22	22	0	0x87C89EF75	60	28	1	0x5AAE39B00	98	2	2	0xADD9E3F88
23	23	0	0x207AA794C	61	29	1	0x138069E54	99	3	0	0x2C1C857DC
24	24	0	0x6A4D1C403	62	30	1	0x966707005	100	4	1	0xCFB4B5503
25	25	0	0x7761B4BD7	63	31	1	0xA5037759E	101	5	2	0xCD8505E21
26	26	0	0x31ABBF06D	64	0	2	0x3FE158D96	102	6	0	0x82892F4CE
27	27	0	0x69C6E455F	65	1	2	0xAED3B839F	103	7	1	0x3979FD176
28	28	0	0xAB3B3CFF0	66	2	2	0xF5AE23268	104	8	2	0x5FA49C311
29	29	0	0x731412685	67	3	2	0x1895E68BE	105	9	0	0xBA7857B19
30	30	0	0xA3135C034	68	4	2	0x1443C94EC	106	10	1	0xBC030C4CA
31	31	0	0xFECCB2B85	69	5	2	0x929547307	107	11	2	0x517F3CBD6
32	0	1	0xAA37BDA7C	70	6	2	0xA17D3230C	108	12	0	0x7E545BE73
33	1	1	0x90955CE1F	71	7	2	0xD54FC0C33	109	13	1	0xDDCA69C3F
34	2	1	0xADBC1B844	72	8	2	0xAB77F079C	110	14	2	0xA01A2C8C7
35	3	1	0xA04A3B197	73	9	2	0xC3CA00A66	111	15	0	0x1C0B64435
36	4	1	0x015E56CB3	74	10	2	0x025519879	112	16	1	0x330282DF2
37	5	1	0x64D6F4038	75	11	2	0x6CF39F815	113	17	2	0x147FCCF4B

2.3 Blind Demodulation of OFDMA Signals

This section is concerned with the required steps to perform blind demodulation of OFDMA signals. Blind demodulation is required in this work as it enables jamming BDA. In this work blind demodulation is considered the process of an uncooperative observer demodulating a pass band OFDMA signal to the information symbols contained on the SCs with no prior knowledge. Blind demodulation is performed on a TDD DL sub frame for varying number of symbols. To perform blind demodulation various OFDMA modulation parameters must be estimated. In the following subsections the pass band OFDMA signal is introduced followed by the techniques required to blindly demodulate the signal to SC information symbols.

2.3.1 Pass Band OFDMA Signal Definition.

The two methods of digital communication transmission are baseband and passband. In this thesis base band signaling has frequencies which measure from 0 Hz to highest signal frequency. Pass band signaling refers to a base band signal which has been translated to a higher frequency, or carrier frequency, prior to transmission and at the receiver is translated back to base band. When translating the base band signal to pass band it is important to reduced ISI. ISI is reduced typically by pulse shaping which involves up sampling and filtering the signal prior to mixing it with the carrier frequency.

Although the vast majority of real wireless communication signals are pass band signals, typically when simulating wireless communication systems it is common to implement base band signal models. This is as the sampling rate required to represent the signal at base band is lower then that of a pass band signal due to the Nyquist Sampling Criterion. Base band simulations are acceptable for a cooperative receiver scenario as the carrier frequency and the pulse shaping, which are required to demodulate the signal, would be known to the receiver. In this case the original base band signal can be easily obtained and simulating a pass band communication system would only increases computational complexity. However, this research is focused on blind demodulation of OFDMA signals where the carrier frequency and pulse shaping are unknown and must be estimated. For this reason a pass band OFDMA signal at an Intermediate Frequency (IF), to reduced the required sampling rate and therefore computational complexity, is considered in this research.

The pass band OFDMA signal is generated by pulse shaping and mixing with the carrier frequency. To minimize ISI the OFDMA base band signal must up sampled so that the pass band sampling period meets the Nyquist Sampling Criterion. The required up sampling rate can be found as the ratio of the required pass band sampling period and base band sampling period. The pass band sampling period can be defined as

$$T_{PB} = \frac{1}{f_c + \frac{\text{OFDMA}_{\text{BW}}}{2}}. \tag{2.14}$$

where OFDMA_{BW} is the passband OFDMA signal BW and f_c is the carrier frequency. Then, if the base band sampling period is T_S the required up sampling rate, L, is

$$L = \left\lceil \frac{T_{PB}}{T_S} \right\rceil. \tag{2.15}$$

where $\lceil \cdot \rceil$ is the ceiling operator. Given the up sampling rate the base band OFDMA time sequence $x[n]$, sampled at T_S, can be up sampled as $x_L[n]$ which is comprised of the original samples of $x[n]$ separated by $L-1$ zeros. The pulse shaped signal is then

$$x_{PS}[n] = \sum_i x_L[i]h[n-i], \tag{2.16}$$

where h is the pulse shaping filter used at the transmitter and group delay is removed. The pass band transmitted signal following mixing with the carrier frequency is then

$$s[n] = x_{PS}[n] \cdot e^{-j2\pi f_c n}. \tag{2.17}$$

Assuming a perfect channel the received pass band pulse shaped over sampled signal is

$$r_{PS,OS}[n] = s[nT_R] + \omega[n], \tag{2.18}$$

where T_R represents the receiver sampling period and ω is Additive White Gaussian Noise (AWGN). The receiver over sampling rate is the rate which the transmitted pass band OFDMA signal is oversampled. The receiver sampling period is defined as in blind demodulation the transmitter sampling period is unknown. For this work it is assumed that that $T_R > 2 \cdot T_S$ which enables the estimation of the transmitter's base band sampling period discussed later in this sub section.

It is important to note that, though cumbersome, the state of pulse shaping and oversampling of the received signal using subscripts are detailed throughout the following process as they must be correctly removed to demodulate the signal.

2.3.2 Carrier Frequency Estimation.

The carrier frequency must be estimated to translate the pass band OFDMA signal to base band where it can be demodulated. Coarse estimation of a carrier frequency is not widely explored in the literature as predominantly research is concerned with cooperative systems where the carrier frequency is approximately known, and design of methods to estimate carrier frequency may be considered trivial.

A simple carrier frequency estimator is derived with the assumption that the pass band signal is symmetric about the carrier frequency and is the only signal in the frequency window of interest. If this is the case the carrier frequency will exist as the center frequency of the detected signal BW. The estimator is then

$$\hat{f}_c = \frac{f_{up} - f_{low}}{2} + f_{low}, \tag{2.19}$$

where f_{up} and f_{low} are the upper and lower frequencies of the signal detected using a simple threshold where signal frequency elements are greater then the noise floor and $\hat{f}_c$ is the estimated carrier frequency.

The carrier frequency can be estimated utilizing the proposed carrier frequency estimator, however, to simplify this work it is assumed that the carrier frequency is estimated with a maximum error of half the SC spacing. The received base band pulse shaped over sampled signal can then be found by removing the carrier frequency as

$$y_{PS,OS}[n] = r_{PS,OS}[n] \cdot e^{j2\pi \hat{f}_c n}. \tag{2.20}$$

With the frequency estimation error a frequency offset exists as $f_{\text{offset}} = \hat{f}_c - f_c$. This frequency offset is known as CFO and it degrades the ability to demodulate the signal. For OFDM and OFDMA signals the CFO is typically normalized and expressed as [6]

$$\epsilon = \frac{f_{\text{offset}}}{\Delta f}, \tag{2.21}$$

where Δf is the SC frequency spacing. Significant research is dedicated to estimation of CFO as it exists in cooperative systems from the frequency differences of the transmitter and receiver's local oscillators. The CFO will be estimated in Section 2.3.6. A fixed carrier phase offset and phase jitter may also exist, however, this can be considered to contribute to the magnitude of the CFO [2]. The received base band pulse shaped oversampled signal with CFO is

$$y_{PS,OS}[n] = x_{PS}[nT_R] \cdot e^{j2\pi n T_R \frac{\epsilon}{N_b}} + \omega[n]. \tag{2.22}$$

2.3.3 Sampling Rate Estimation.

To perform blind demodulation the transmitter sampling period, T_S, must be estimated. The literature presents a variety of methods to determine the sampling period by exploiting certain signal properties and include use of signal BW [7], wavelet transforms [8], IFFT [9], filter banks [10], and cyclostationarity [11, 12, 13]. Some of these methods, such as the IFFT method, are only applicable for single carrier signals while others do not consider pulse shaping or are significantly more complex. The method used within this research exploits the cyclostationary properties of the oversampled OFDMA signal. A cyclostationary process is a signal having statistical properties that vary cyclically with time. A property of cyclostationary signals is that they arise as a result of oversampling digital communication signals where the non zero positive cyclic frequency will be $\alpha_0 = \frac{T_S}{T_R}$ [11]. The up sampling performed to translate the base band signal to pass band does not impact the estimate of the sampling period, T_S, as it only increases oversampling. Consequently, cyclostationary properties can be exploited to estimate the T_S. Recall the pulse shaped oversampled signal, with $\epsilon = 0$ to simplify derivation, is

$$y_{PS,OS}[n] = x_{PS}[nT_R] + \omega[n]. \tag{2.23}$$

The discrete time cyclic autocorrelation function, $\hat{R}_D^{\alpha}(\tau)$, for cyclic frequency α is then [11]

$$\hat{R}_D^{(\alpha)}(\tau) = \frac{1}{D}\sum_{n=0}^{D-1} y_{PS,OS}[n+\tau]y^*_{PS,OS}[n]e^{-j2\pi\alpha n}, \tag{2.24}$$

where D is the number of samples and * is the complex conjugate. Now let [11]

$$\hat{\mathbf{R}}_D^{(\alpha)} = \left[\hat{R}_D^{(\alpha)}(0)\cdots\hat{R}_D^{(\alpha)}(N)\right], \tag{2.25}$$

where N is the number of cyclic correlation coefficients taken into account. $N = 11$ is used for this research. The estimate of α_0 is then [11]

$$\hat{\alpha}_0 = \arg\max_{\alpha} ||\hat{\mathbf{R}}_D^{(\alpha)}||, \tag{2.26}$$

where the search interval is $0 < \alpha \leq \frac{1}{2}$. The estimated sampling period is then

$$\hat{T}_S = \hat{a}_0 T_R. \tag{2.27}$$

It is important to note that this estimator requires significant computational complexity. Further, it suffers when α near 0, however, Mazet and Loubaton overcome this by utilizing a weighted version of this estimator [11]. The weighted estimator is not implemented due to its increased complexity, and the sub optimal estimator is considered to meet the goals of this research.

2.3.4 Pulse Shaping Filter Roll Off Factor Estimation.

To demodulate the signal the pulse shaping filter at the transmitter must be known or estimated in the non cooperative environment. Firstly, this work assumes that a raised cosine filter is used which consists of a root raised cosine filter at the transmitter and receiver. This is a valid assumption as these filters are widely employed because they are practical to implement in wireless communication systems. The advantage of assuming a raised cosine filter is they only have one variable, the roll off factor, that must be estimated following the estimation of the sampling period in previous steps. In the literature the estimation of the pulse shaping filter is not widely studied. In [14] a method is presented using the IFFT and least squares to estimate the roll off factor. The author of [15] exploits the property that the raised cosine pulse is a matched filter and when the correct roll off is used the Signal to Noise Ratio (SNR) will be maximized. Another method is explored in [16] where second order cyclostationarity is exploited to estimate the roll off factor. This research adopts and extends methods used in [15] due to its simplicity to implement while remaining robust. Let the continuous raised cosine filter be defined as

$$H_{RC}(f) = \begin{cases} T, & |f| \leq \frac{1-\alpha}{2T} \\ \frac{T}{2}\left[1 + \cos\left(\frac{\pi T}{\beta}\left[|f| - \frac{1-\beta}{2T}\right]\right)\right], & \frac{1-\beta}{2T} < |f| \leq \frac{1+\beta}{2T} \\ 0, & \text{otherwise,} \end{cases} \tag{2.28}$$

where β is the roll off factor and T is the sampling period. The root raised cosine filter, H_{RRC}, used at the transmitter and receiver is

$$|H_{RRC}(f)| = \sqrt{|H_{RC}(f)|}, \tag{2.29}$$

or

$$H_{RC}(f) = H_{RRC}(f) \cdot H_{RRC}(f). \tag{2.30}$$

From this definition if a root raised cosine filter is employed at the transmitter, the matched filter will be a root cosine filter with the same parameters at the receiver. This can be exploited to estimate β as a matched filter, in the presence of AWGN, will maximize the SNR of the output signal. The estimator can then be defined using Parseval's energy theorem, using a discrete raised cosine filter, and assuming no CFO as

$$\hat{\beta} = \arg\max_{\beta}\left(\sum_{n}\left|\sum_{i} y_{PS,OS}[i]h_{RRC}^{(\beta)}[n-i]\right|^{2}\right), \tag{2.31}$$

where the search interval is $0 < \beta \leq 1$, $h_{RRC}^{(\beta)}$ is the time domain root cosine filter at the receiver defined for a β and sampling period $\hat{T}_S$. It is important to note that when defining the discrete raised cosine filter that the frequency resolution factor and number of filter taps must be defined, however, their magnitude affects only the accuracy of the estimate. Further, for this estimator to be effective it is required that $\hat{T}_S$ is an accurate estimate. The oversampled received base band signal is then

$$y_{OS}[n] = \sum_i y_{PS,OS}[i] h_{RRC}^{(\hat{\beta})}[n-i], \tag{2.32}$$

where $\hat{\beta}$ is the estimated filter roll off factor and the signal is corrected for filter group delay. The base band signal can now be found by down sampling by the estimated sampling rate as

$$y[n] = y_{OS}[n\hat{T}_S], \tag{2.33}$$

where it is assumed that the signal is oversampled by an integer. In the case where the oversampling rate is not an integer the signal could be resampled at the correct sampling period.

2.3.5 Synchronization Parameter Estimation.

In the ideal case the signal at this stage is at base band, and is sampled at the correct rate with no CFO. To demodulate the OFDMA signal to SCs the synchronization parameters must be estimated which in samples are the symbol length N_b, cyclic prefix length N_G and symbol delay θ. The literature has widely explored blind estimation of synchronization parameters by exploiting the cyclostationarity of OFDM signaling due to the CP extension [16, 17, 18, 19, 20] where variation exists due to assumptions of known parameters. This research adopts and extends methods described in [19] for the proposed sub optimal estimator. This work is chosen as the assumptions are aligned with this stage of the blind estimation process and the described estimators can be simplified via previously estimated parameters. The first step of the estimation process is to find N_b by exploiting repetition due to CP. The discrete correlation of the received signal is [19]

$$R_y[\tau] = \sum_{i=1}^{D-\tau} y[i]y^*[i+\tau], \tag{2.34}$$

where D is the number of samples. Assuming statistical averaging the correlation can be obtained as [19]

$$R_y[\tau] = \begin{cases} \sigma_S^2 + \sigma_\omega^2, & \tau = 0 \\ \frac{N_G}{N_b+N_G}\sigma_S^2, & \tau = N_b \\ 0, & \text{otherwise,} \end{cases} \tag{2.35}$$

where σ_S^2 and σ_ω^2 are the signal and noise variances. Note that when $\tau = N_b$ the autocorrelation is the signal power of the CP. By exploiting this property the delay of the maximum of the autocorrelation, for correlation delays $\tau > 0$, will yield N_b as [19]

$$\hat{N}_b = \arg\max_{\tau>0} \left(\left| R_y[\tau] \right| \right), \tag{2.36}$$

As the signal is sampled at the correct rate the typical FFT sizes employed in OFDMA are the possible values of N_b. The estimator complexity is then reduced in by bounding the autocorrelation delays searched to these possible FFT sizes. The FFT sizes assumed in this research are 64, 128, 256, 512, 1024, and 2048.

Following estimation of N_b the CP duration and delay θ can be found by testing for different N_G values. In order to reduce the complexity of the estimator we can assume the standard CP orders are employed which are $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{16}$, $\frac{1}{32}$ [1]. This bounds the search values to $N_G = \lceil \frac{1}{4}\hat{N}_b \rceil, ..., \lceil \frac{1}{32}\hat{N}_b \rceil$. Further, the delay can be bounded by the symbol duration $\theta = 0, 1, ..., \hat{N}_b - 1$. The joint estimator exploits that the maximum correlation between only the CP samples and their copy will occur for the correct delay and CP length. This correlation is performed for all possible OFDMA symbols for a given CP length. The estimator is defined as [19]

$$\hat{N}_G, \hat{\theta} = \arg\max_{N_G,\theta} \left(\left| \sum_{m=0}^{\lfloor \frac{D}{N_b+N_G} \rfloor} \sum_{p=1}^{N_G} y\left[m\left(\hat{N}_b + N_G\right) + p + \theta \right] \cdot y^* \left[m\left(\hat{N}_b + N_G\right) + \hat{N}_b + p + \theta \right] \right| \right), \tag{2.37}$$

where $\lfloor\cdot\rfloor$ is the floor of the number of possible symbols considering the tested signal length.

Following the estimation of the symbol parameters, the number of received OFDMA symbols, N_{Sym}, can be estimated and the signal can be corrected for delay and demodulated. However, at this stage the assumption of no CFO is not valid and consequently it must be estimated.

2.3.6 CFO Estimation.

Until this stage we have ignored CFO, however, this is not a valid assumption as CFO will exist due to carrier frequency estimation, local oscillator offsets and Doppler shift. If we do not estimate the CFO the ability to demodulate the signal will be degraded. In literature CFO estimation is performed in either the time or frequency domain [6]. Methods include exploiting the CP [6, 21], a specialized training sequence [22, 23], and cyclostationarity [16, 24]. A time domain technique exploiting the CP is detailed in [6]. The methods utilizing training sequences cannot be implemented in this research as the sequence is unknown. Further, the work completed in [21] assumes knowledge of the SNR which is not suitable for this research. The cyclostationarity method used in [16] could be employed however does not provide significant improvement over the simpler CP method employed in [6]. Consequently, the time domain CP method is used within this research utilizing a extension of the method performed in [6]. The method exploits that under negligible channel effects the phase difference between the CP and the corresponding rear part of the OFDM symbol, spaced N_b samples apart, caused by CFO ϵ is $2\pi N_b\epsilon/N_b = 2\pi\epsilon$. Then, the CFO can be estimated as the mean phase angles between the product of the CP samples and the corresponding rear samples for all OFDMA symbols as

$$\hat{\epsilon} = \frac{1}{2\pi}\arg\left(\sum_{n=0}^{N_{Sym}}\sum_{m=-N_G}^{-1} y_\epsilon^*[n+m]y_\epsilon[n+m+N_b]\right), \tag{2.38}$$

where y_ϵ is the received base band signal with CFO found following down sampling in the previous section and ϵ is normalized CFO. Since the arg() operator is performed using $\tan^{-1}()$, the range of the CFO estimation is bounded by $\frac{1}{2\pi}\cdot\pm\pi = \pm0.5$ so that $|\hat{\epsilon}| < 0.5$.

The estimator's performance increases for increased number of symbols, however, the number of symbols used to estimate the CFO must be limited according to the rate of change of the channel. It is assumed in this work that the major weight of the CFO is due to the estimation error of the carrier frequency, while CFO from the channel is less significant, and in this case the whole length of the DL sub frame is utilized to estimate the CFO. In a channel which varies more rapidly it may be beneficial to first estimate and correct the CFO due to carrier frequency estimation from multiple symbols or DL frames and subsequently decrease the number of symbols to estimate the CFO due to the varying channel.

At this stage the CFO can be removed from the signal as

$$y[n] = y_{\epsilon}[n] \cdot e^{-j2\pi n \frac{\hat{\epsilon}}{\hat{N}_b}}. \tag{2.39}$$

The signal can now be demodulated to access the transmitted information such as the burst profile.

2.4 Jamming BDA via observation of Link Adaptation

LA is a mechanism where communication systems can adapt according to channel conditions in order to enable better utilization of available resources. There are typically three methods of LA which are adaptive modulation, adaptive FEC and Automatic Repeat Request (ARQ) [25]. In adaptive modulation the transmitter and receiver negotiate according to the channel conditions to set the most BW efficient signal constellation. This involves a reduction of the modulation order as interference increases, for example QPSK to BPSK. Adaptive FEC adds overhead to the transmitted data in the form of FEC code words of increased length as interference increases. ARQ involves retransmissions of packets which are unacknowledged where retransmissions cause a reduction in overall throughput.

Communication systems may employ a combination of the above schemes. As a goal of this research is to perform jamming BDA this research exploits the adaptive modulation, employed by OFDMA systems, to classify the success of jamming effectiveness. The research classifies successful jamming when the adaptive modulation changes order over subsequent frames indicating higher interference levels as seen by the transmitter and receiver. As OFDMA signals may vary the modulation of SCs differently, as the channel effects are not typically uniform over the signal BW, the modulation of each SC must be monitored rather than a single modulation for all SCs. In a cooperative OFDMA scenario, or where the OFDMA modulation scheme is a specified standard, the change of SC modulation order can determined though the demodulated signal's burst profiles which provide modulation signaling. However, in the case where the burst profile is not available, such as a in military signal, the SC modulation type must be classified through different means. The following section outlines the classification of SC modulation of OFDMA signals.

2.4.1 Classification of SC Modulation.

Classification of OFDM and OFDMA SCs has not been widely studied. Research has been performed, in the cooperative case, with the motivation to increase throughput of adaptive modulation systems by removing the requirement of modulation signaling. These methods can not be used in the non cooperative scenario as they rely on a priori knowledge of the SNR bounds for modulation change [26, 27] and coding [28]. Fortunately, Automatic Modulation Classification (AMC) has been widely studied to determine the presence of wireless communications including single carrier modulation schemes, OFDM and OFDMA signals. This research can be applied to determine SC modulation by considering the successive modulated symbols on a OFDMA SC to be time domain samples. AMC can then be applied on these sequences of samples to determine the modulation type. However, care must be taken when considering the properties of the AMC techniques as unlike single carrier modulated signals, noise and channel affect the successive time domain OFDMA samples rather than the modulated symbols which exist on the frequency domain SCs on successive OFDMA symbols.

AMC is typically approached through two methods which involve pattern recognition [2, 29, 30] and decision theoretic approaches [31, 32]. Pattern recognition methods are typically less complex and do not perform as well as decision theoretic approaches [33]. However, when implemented correctly, some pattern recognition methods are near-optimal [33]. To identify the modulation on the OFDMA SCs this research utilizes a statistical pattern recognition technique that classifies modulation type with sixth order cumulants [2]. This method is chosen due to near optimal performance, it can perform with carrier frequency and phase offsets, and it is simple to implement. Further, this method employed is not adept in multi-path, however, it may extended to perform blind equalization and modulation classification using techniques such as [34].

Firstly let the sequence of received samples on a SC over successive OFDMA symbols be $m[n]$. Then for a complex valued stationary process, conditions met by $m[n]$ as it is a sequence of samples with a fixed modulation yielding constant mean and variance over time, the second order moment can be defined in two ways depending on the conjugation [2]

$$C_{20} = E\left[m^2[n]\right], \tag{2.40}$$

and

$$C_{21} = E\left[|m[n]|^2\right], \tag{2.41}$$

where $E[\cdot]$ is the expectation. Similarly the fourth and sixth order cumulants can be defined as [2]

$$C_{40} = cum\left(m[n], m[n], m[n], m[n]\right), \tag{2.42}$$

$$C_{41} = cum\left(m[n], m[n], m[n], m^*[n]\right), \tag{2.43}$$

$$C_{42} = cum\left(m[n], m[n], m^*[n], m^*[n]\right). \tag{2.44}$$

$$C_{63} = cum\left(m[n], m[n], m[n], m^*[n], m^*[n], m^*[n]\right). \tag{2.45}$$

For the zero mean modulated signal the *cum*() is defined by the joint cumulant formula

$$cum(x_1, ..., x_n) = \sum_{\pi}(|\pi| - 1)!(-1)^{|\pi|-1} \prod_{B\in\pi} E\left(\prod_{i\in B} X_i\right), \tag{2.46}$$

where π runs through the list of all partitions of $\{1, ..., n\}$, B runs through the list of all blocks of the partition π, and $|\pi|$ is the number of parts in the partition. For example the fourth order cumulant is defined as

$$cum(wxyz) = E(wxyz) - E(wx)E(yz) - E(wy)E(xz) - E(wz)E(xy). \tag{2.47}$$

The cumulants above can be estimated from the sample estimates of each moment. As $m[n]$ is zero mean, due to no DC offset, the sample estimates are [2]

$$\hat{C}_{20} = \frac{1}{N}\sum_{n=1}^{N} m^2[n], \tag{2.48}$$

$$\hat{C}_{21} = \frac{1}{N}\sum_{n=1}^{N} |m[n]|^2, \tag{2.49}$$

where N is the number of samples. This leads to [2]

$$\hat{C}_{40} = \frac{1}{N}\sum_{n=1}^{N} m^4[n] - 3\hat{C}_{20}^2, \tag{2.50}$$

$$\hat{C}_{41} = \frac{1}{N}\sum_{n=1}^{N} m^3[n]m^*[n] - 3\hat{C}_{20}\hat{C}_{21}, \tag{2.51}$$

$$\hat{C}_{42} = \frac{1}{N}\sum_{n=1}^{N} |m[n]|^4 - \left|\hat{C}_{20}\right|^2 - 2\hat{C}_{21}, \tag{2.52}$$

$$\hat{C}_{63} = \frac{1}{N}\sum_{n=1}^{N} m[n]^3 m^*[n]^3 - 9\hat{C}_{42}\hat{C}_{21} - 6\hat{C}_{21}^3. \tag{2.53}$$

As the second moment $\hat{C}_{21}$ is the average power of the signal, the cumulants are typically normalized as [2]

$$\hat{C}_{4k} = \frac{\hat{C}_{4k}}{\hat{C}_{21}^2} \quad k = 0, 1, 2; \tag{2.54}$$

and

$$\hat{C}_{63} = \frac{\hat{C}_{63}}{\hat{C}_{21}^3}. \tag{2.55}$$

Table 2.3: Theoretical cumulant statistics C_{40}, C_{42}, C_{63} for OFDMA constellation types extended using [2]

Constellation	$\|C_{40}\|$	C_{42}	C_{63}
BPSK	2	-2	16
QPSK	1	-1	4
QAM-16	0.68	-0.68	2.08
QAM-64	0.62	-0.62	1.797
Null	0	0	0

For this research it is assumed that the average power of the modulated SC is 1 and hence normalization is not required. Following the derivation of the cumulants their theoretical values must be found for the possible modulation types. As the modulation types used in OFDMA are defined as BPSK, QPSK, QAM-16 and QAM-64 [1] we must only consider these cumulants. Further, the SC classification process must also be able to classify the null carriers. In Table 2.3 the theoretical values of the cumulants are obtained by computing the expectation of the signal in noise free scenario with unit energy [2]. The value for the null carrier is zero as all its moments are zero.

By considering the cumulants, a classifier should have the greatest performance using C_{63} as decision space between the theoretical cumulants is the largest. By assuming that the variance of C_{63} for all modulation types is the same, in fact [2] proves that they are distributed similarly, a Maximum Likelihood (ML) classifier can be devised to determine the modulation type. The decision regions of the classifier are defined as the mid value between each successive constellation's value, except for between BPSK and QPSK, of C_{63}. The mid point is not selected between BPSK and QPSK as BPSK is distributed differently. For the other modulation cumulants it is assumed equal distribution. The ML classifier in this work is then defined as

$$\begin{array}{lr}
\infty > \hat{C}_{63} \geq 6, & \text{Choose BPSK} \\
6 > \hat{C}_{63} \geq 2.75, & \text{Choose QPSK} \\
2.75 > \hat{C}_{63} \geq 1.9385, & \text{Choose QAM-16} \\
1.9385 > \hat{C}_{63} \geq 0.8985, & \text{Choose QAM-64} \\
0.8985 > \hat{C}_{63} \geq -\infty, & \text{Choose Null}
\end{array} \tag{2.56}$$

From the defined classifier it is apparent that it should perform well in distinguishing between PSK and QAM. However, due to the small decision regions differentiating QAM modulation types it can be expected that the classifier may not perform as well when classifying between QAM modulation types.

2.5 Related Work

The blind estimation of OFDM parameters has been widely studied in literature [19, 20, 21, 22, 23, 26] most of which focused on the synchronization parameters or on one or two other parameters. Work which considers a more complete blind estimation scheme is far more limited. In [17, 18] modulation parameters are estimated with a known sampling frequency and assumption that the carrier frequency and pulse shaping are known. These works do consider estimating CFO. Much of this work makes assumptions of known parameters as they are for cooperative systems. Less works exists where a non cooperative scenario is assumed and all modulation parameters are estimated. The work by [7] attempts blind parameter estimation including sampling rate, however, estimation of CFO and pulse shaping is ignored and the sampling rate estimator is not robust. The most complete blind classification method for OFDM is described by Shi in [13, 16] and is the work on which a portion of the blind parameter estimation in this research is based. There are no works found to date which combine the estimators employed to perform blind demodulation in this research, however, the employed estimators are considered by other research in isolation with varied assumptions. Although blind parameter estimation is detailed in all the above works none consider OFDMA signals or perform SC classification enabling BDA or demodulation. To a certain extent it is a valid assumption that classification of modulation type is not required as modulation signaling will be available once the base band signal and synchronization parameters are estimated. However, this would not be the case for many systems that uncooperative blind demodulation is performed, like military systems, which would not conform to civilian modulation standards in order to protect transmitted information. The estimation of the SC modulation for these cases is a goal of this research.

It is important to note, as discussed in Section 2.4.1, that methods have been studied to classify SC modulation type in the absence of modulation signaling for OFDM signals. These methods, however, are in the cooperative scenario where synchronization parameters are known [26, 27, 28] and mostly based on estimating SNR with knowledge of LA thresholds. These methods are performed to improve throughput of link adaptive OFDM wireless communication systems by removing the requirement of modulation signaling.

The majority of work concerned with estimating synchronization parameters and classifying modulation consider only OFDM and not OFDMA. This is as OFDMA signals are very similar to OFDM signals and the methods employed to estimate parameters for OFDM signals generally operate for OFDMA. There are however significant frame differences and differences in pilot modulation [1] whose influences can be explored. Some related work is concerned with the estimation of OFDMA parameters is to classify OFDM and OFDMA systems using pilot induced cyclostationarity [35]. In [36] a parameter estimation scheme for OFDMA signals is devised which is capable of signal demodulation. This scheme however ignores the CFO and pulse shaping.

There are no works found to date that observe LA to perform BDA.

III. Methodology

This chapter introduces the simulation models proposed to generate the pass band OFDMA signal, blindly demodulate the OFDMA signal and perform BDA via observing LA. Each model is broken into a series of blocks for which implementation and independent performance is detailed. Each model is based on the theory presented in Chapter II under similar headings. The performance of the complete model is analyzed in Chapter IV in different channel conditions. The employed channels are also introduced in this chapter. All simulation is performed in MATLAB® [37].

3.1 OFDMA Signal Generation Model

Figure 3.1 presents the model which generates the simulated OFDMA signal. Blocks present each important stage required to generate the OFDMA signal and are labeled with the input and output parameters. Each model block is implemented according to the theory discussed in Chapter II. For all simulations the signal is generated with a size 128 FFT for a single TDD DL sub frame using DL-PUSC. The size 128 FFT is used as it reduces computational complexity and has the least number of samples available to estimators. As estimator performance is largely based on the number of samples per OFDMA symbol the lowest FFT size, for a fixed number of symbols in a DL sub frame, is expected to have minimum performance. As detailed Section 2.2.2 the TDD frame structure is employed in the simulation as it is the most widely used in practical OFDMA systems. Further, DL sub frame lengths of 25, 75, and 250 symbols are considered as they represent possible DL sub frame lengths in practical OFDMA implementations. The pulse shaping block performs both up sampling and filtering of the OFDMA signal to prevent ISI. The channel models used in this work are a perfect channel and single multi-path which is defined in Section 3.2. To evaluate the individual performance of the developed estimators and

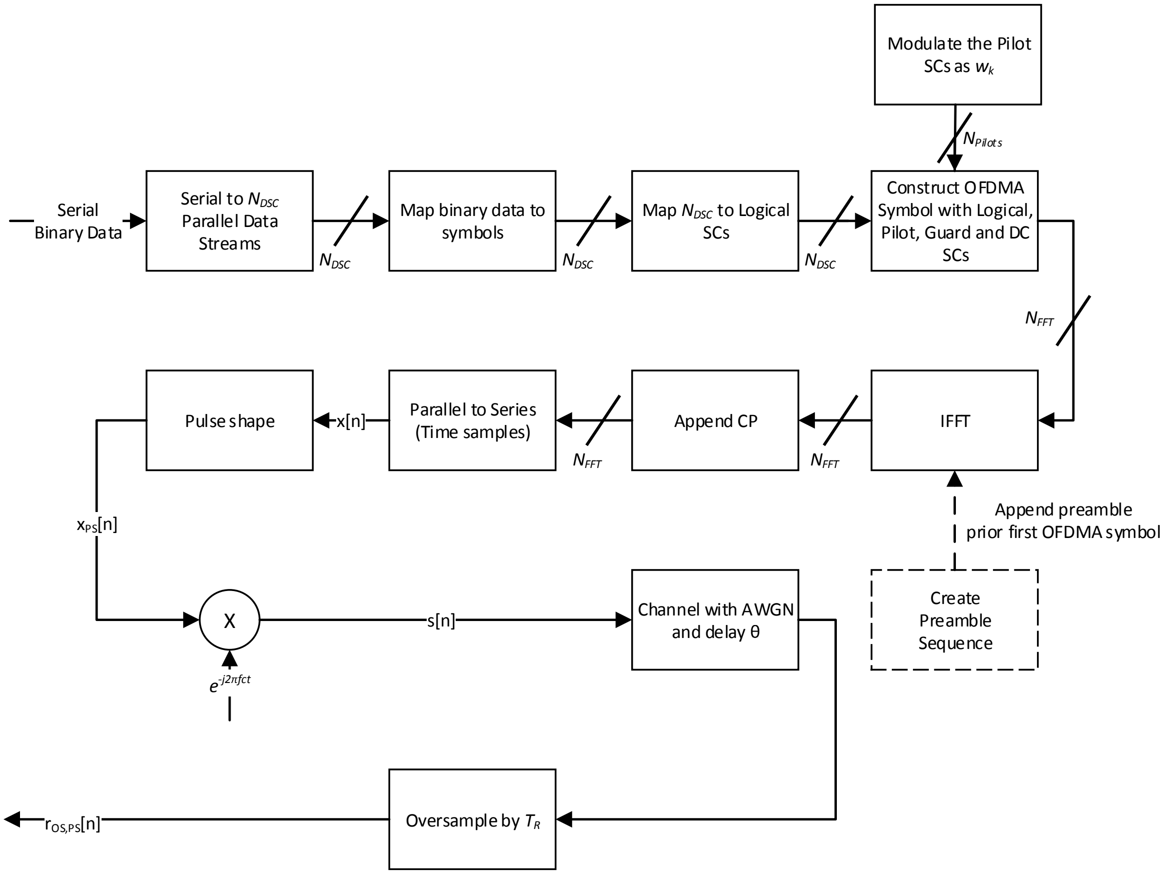

Modulate the Pilot SCs as w_k
N_{Pilots}
Serial Binary Data
Serial to N_{DSC} Parallel Data Streams
N_{DSC}
Map binary data to symbols
N_{DSC}
Map N_{DSC} to Logical SCs
N_{DSC}
Construct OFDMA Symbol with Logical, Pilot, Guard and DC SCs
N_{FFT}
Pulse shape
x[n]
Parallel to Series (Time samples)
N_{FFT}
Append CP
N_{FFT}
IFFT
Append preamble prior first OFDMA symbol
$x_{PS}[n]$
X
s[n]
Channel with AWGN and delay θ
Create Preamble Sequence
$e^{-j2\pi f c t}$
$r_{OS,PS}[n]$
Oversample by T_R

Figure 3.1: Signal generation model.

classifiers of the blind demodulation and BDA models a perfect channel are simulated in this chapter. The effects of a single multi-path channel are explored in Chapter IV where the complete model performance is evaluated. To simplify simulation computational complexity, by decreasing required sampling rate, an IF OFDMA signal is simulated with a BW significantly smaller then a practical OFDMA system. The results found for the simulated signal are applicable to practical OFDMA signals as the exploited parameters are shared, however, higher sampling rates are required to yield the same results.

The OFDMA signal generation model requires some measure of validation. A suitable method is to find the model Bit Error Rate (BER) for the possible SC modulation schemes as they can be compared to the theoretical BER of single carrier modulations for each constellation. To find the BER a signal receiver is designed akin to the generation model. To compare the BER for each modulation the SNR as a function of $\frac{E_b}{N_0}$ for a pass band OFDMA symbol is

$$\mathrm{SNR}_{\mathrm{OFDMA}} = 2 \cdot \frac{E_b}{N_0} \cdot (k) \cdot \left(\frac{N_{DSC}}{N_b}\right) \cdot \left(\frac{N_b}{N_b + N_G}\right), \tag{3.1}$$

where the factor of two accounts for the noise variance of the base band signal being double that of the corresponding pass band signal, k is the number of bits per symbol used for SC modulation, the term $\frac{N_{DSC}}{N_b}$ is the ratio of data SC to total number of SC per symbol, and $\frac{N_b}{N_b+N_G}$ is the ratio of symbol extension due to cyclic prefix. To prevent an offset between the theoretical and expected simulation BER the loss of energy due to the CP must be removed, hence, the simulation SNR used in the following simulations is defined as

$$\mathrm{SNR}_{\mathrm{SIM}} = 2 \cdot \frac{E_b}{N_0} \cdot (k) \cdot \left(\frac{N_{DSC}}{N_b}\right). \tag{3.2}$$

With this SNR scaling we can expect the BER of the simulation to be the same as the theoretical for each modulation type.

Figure 3.2 and Figure 3.3 present the simulated and theoretic BER for the OFDMA PSK and QAM modulations respectively with confidence intervals. As the BER are statistically the same the signal generation model is validated. The simulations are performed for a frame with 7500 symbols, with 10 kHz carrier frequency, 5 kHz BW, up sampling rate of 8, over sampling rate of 1, pulse shaping roll off factor of 0.7, and CP ratio of $\frac{1}{4}$. A frame length of 7500 symbols is employed to enable statistical confidence. Other CP ratios are not presented as they do not impact the BER.

Figure 3.4 presents the unnormalized Power Spectral Density (PSD) of a pass band OFDMA DL sub frame of 75 symbols and no AWGN to illustrate the signal BW and carrier frequency. The null frequency can be observed in the mid of the spectrum.

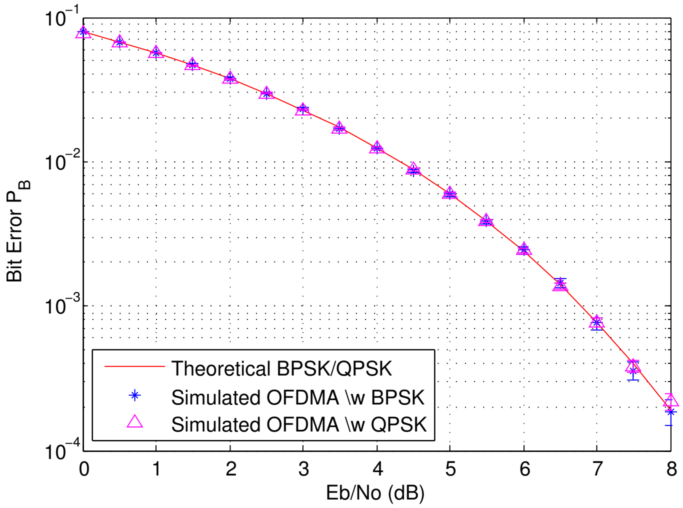


Figure 3.2: Simulated and theoretic BER for PSK modulation types.

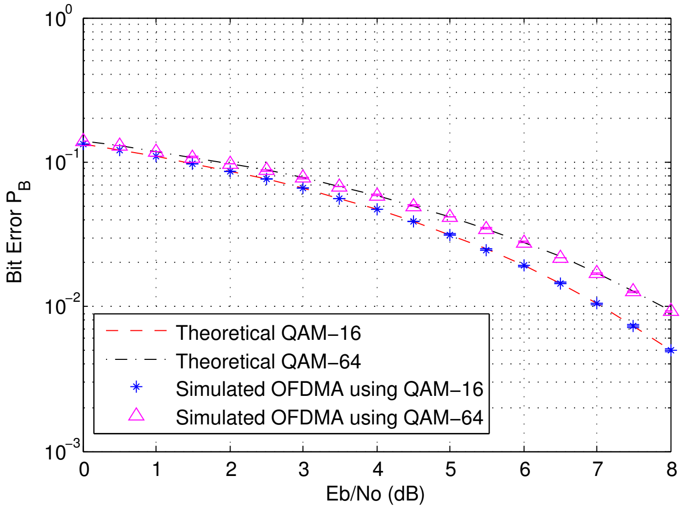


Figure 3.3: Simulated and theoretic BER for QAM modulation types.

3.2 Channel Conditions

This research considers two different Finite Impulse Response (FIR) channel models. The channels considered are a perfect and a simple multi-path. In the case of the perfect channel a non-dispersive channel is used solely to evaluate the performance of the models

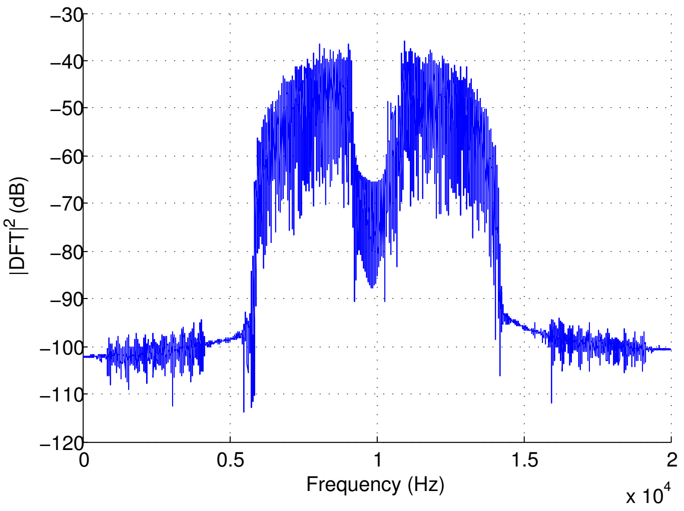


Figure 3.4: Unnormalized one sided PSD of 75 OFDMA symbols using BPSK modulation and 128 FFT.

without channel interference. The perfect channel is defined as

$$h = [1, 0, ..., 0], \tag{3.3}$$

where h is the channel of length $N_G - 1$. The effects of a simple multi-path channel on the OFDMA blind demodulation model and jamming BDA model is considered in Chapter IV. The single multi-path channel is a a dispersive channel and is defined as

$$h = [1, 0, 0, \alpha, 0, ..., 0], \tag{3.4}$$

where α is a value less than 1 and h is the channel of length $N_G - 1$. For this research alpha is defined as $\alpha = 0.5$.

3.3 OFDMA Blind Demodulation Model

Figure 3.5 is the proposed model which performs blind demodulation of the OFDMA signal. The model contains various blocks where the input and output estimated parameters are detailed. The implementation and performance of each estimation block, which are colored red and have a dashed line style, assuming correct input estimated parameters, are

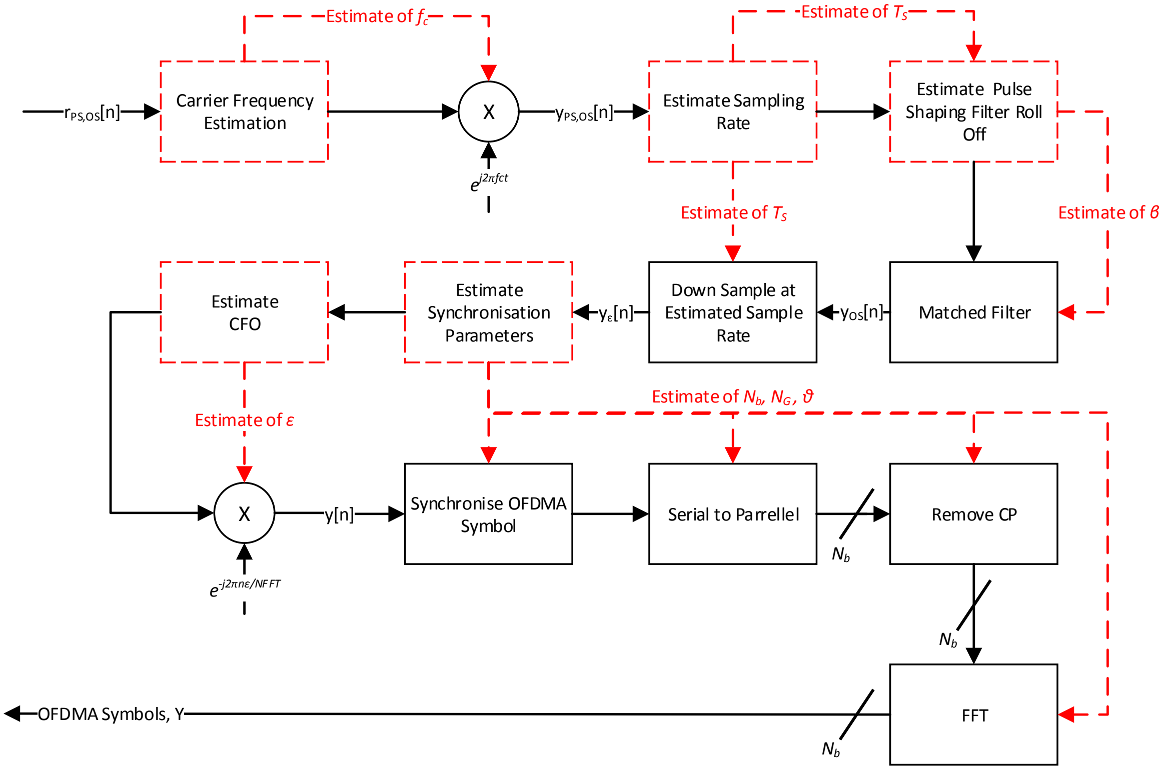


Figure 3.5: Blind demodulation model.

detailed in the following sub sections. The methods of implementing the non estimation blocks are not detailed as they are the mathematical operations introduced in Chapter II.

The signal operated on by the blind demodulation model is generated by the OFDMA signal generation model introduced in the previous section. As the SNR does not vary for modulation type blind demodulation performance is only considered for BPSK SCs in this section's simulations.

3.3.1 Carrier Frequency Estimation.

To perform course carrier frequency estimation a trivial estimator is introduced in Section 2.3.2. To simplify this work it is assumed that the carrier frequency is estimated with a maximum estimation error of half the SC spacing which corresponds to a CFO of

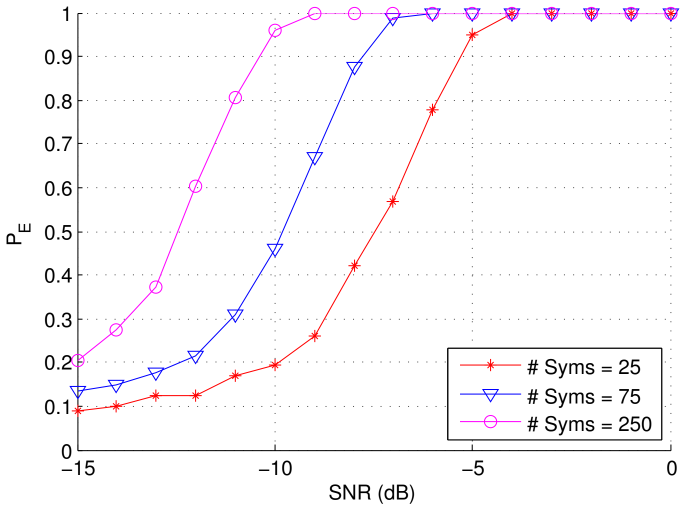


Figure 3.6: Probability of correct estimation of sampling rate.

$|\epsilon| < 0.5$. Half the carrier frequency spacing is used as it the maximum CFO which can be corrected by the CFO estimator.

3.3.2 Sampling Rate Estimation.

The sampling rate estimator is developed as the theory presented in Section 2.3.3. Figure 3.6 presents the performance of the sampling rate estimator. The simulation is performed using a carrier frequency removed signal with varying frame lengths in symbols, 5 kHz BW, up sampling rate of 8, over sampling rate of 1, pulse shaping roll off factor of 0.7, no CFO, and CP ratio of $\frac{1}{4}$. The sampling rate is determined to be estimated correctly when there is zero estimation error. Other CP ratios are not presented as they do not impact the oversampling rate estimation.

To determine the impact of the oversampling rate magnitude Figure 3.7 presents the performance for a fixed SNR of -12.5 dB and varying oversampling rates. All other signal properties are the same as the signal described in the previous paragraph. In Figure 3.7 it can be observed that as the oversampling rate is increased so does the probability of correct estimation. This is due to the increased number of samples that can be used by the

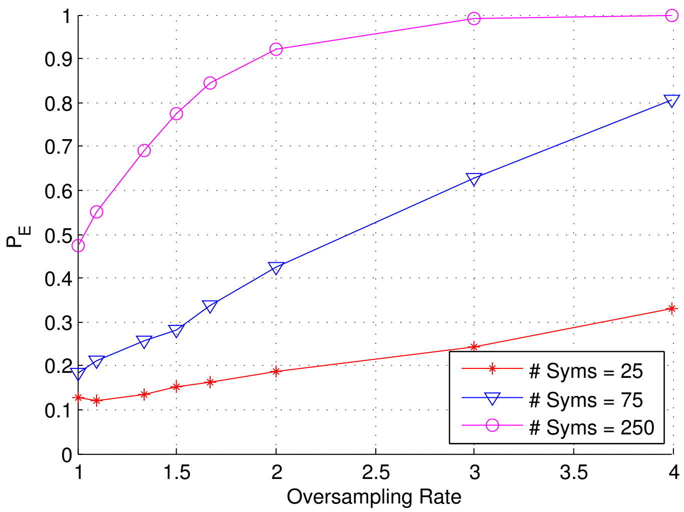


Figure 3.7: Probability of correct estimation of sampling rate for varying oversampling rates.

estimator. It is important to note that increased oversampling causes greater computational complexity.

3.3.3 Pulse Shaping Filter Roll Off Factor Estimation.

The pulse shaping estimator is developed as the theory presented in Section 2.3.4. Figure 3.8 presents the performance of the pulse shaping roll off factor estimator. For performance evaluation of the pulse shaping filter roll off estimator the transmitter sampling period, T_S, is assumed to be estimated correctly. The simulation is performed using a carrier frequency removed signal with varying frame lengths in symbols, 5 kHz BW, up sampling rate of 8, over sampling rate of 1, pulse shaping roll off factor of 0.7, no CFO, and CP ratio of $\frac{1}{4}$. Other CP ratios are not presented as they do not impact the roll off factor estimation.

To determine the impact of the pulse shaping filter magnitude Figure 3.9 presents the estimator's performance for a fixed SNR of 3 dB for varying filter roll off factors. All assumptions and other signal properties are the same as the signal described in the previous

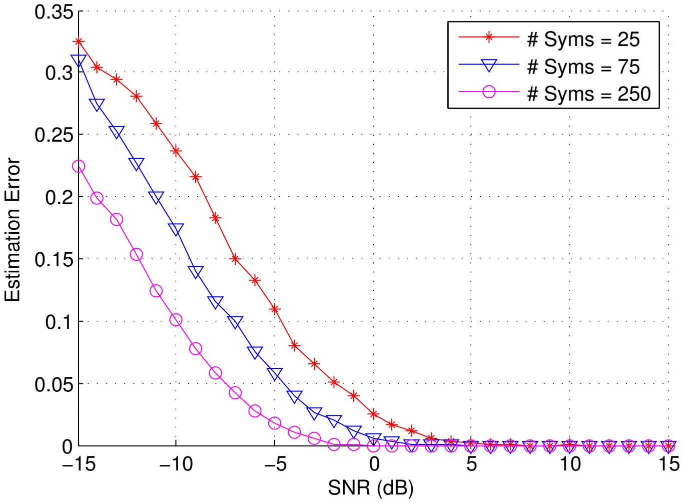


Figure 3.8: Mean absolute estimation error of roll off factor β.

paragraph. It can be noted from Figure 3.9 that the higher the roll off factor the greater the estimation error, however, the estimation error is not significantly different and reduces for greater number of OFDMA symbols per DL sub frame. As there is not a significant increase in estimation error a fixed pulse shaping roll off factor of 0.7 is used in all simulations. The cause of increased estimation error may be due to the matched filter BW increasing with the roll off factor, therefore the filter applies a greater weighting to random noise spectral components beyond the signal bandwidth. These noise spectral components cause the filter maximum output signal power to be less discernible for the estimators defined β search interval increasing estimation error.

3.3.4 OFDMA Synchronization Parameter Estimation.

The synchronization parameter estimator is developed as the theory presented in Section 2.3.5. Figure 3.10, Figure 3.11 and Figure 3.12 present the probability of estimating the synchronization parameters N_b, N_G, and θ. The simulation uses a received base band, down sampled and matched filtered signal for varying frame lengths in symbols. The

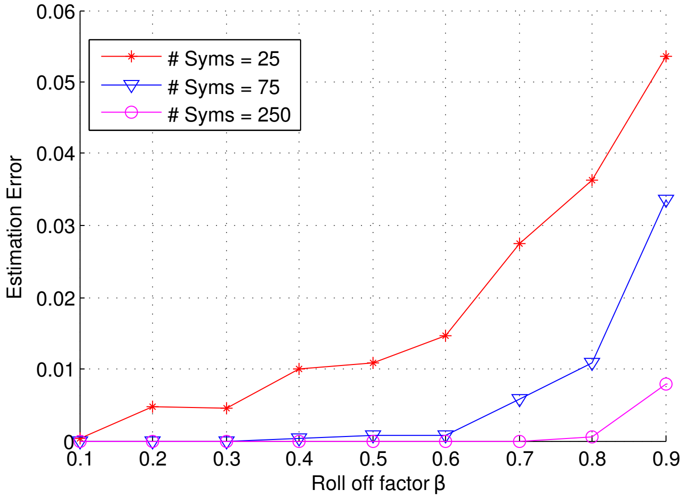


Figure 3.9: Mean absolute estimation error of roll off factor β for varying β.

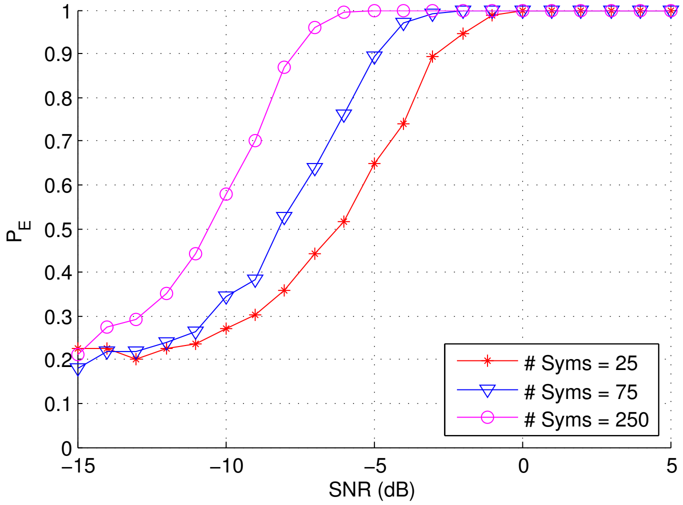


Figure 3.10: Probability of correct estimation of symbol length N_b.

signal is generated with no CFO, a CP ratio of $\frac{1}{4}$ and random delay drawn from a uniform distribution on the interval $\{\theta \,|\, 0 \geq \theta < N_b\}$

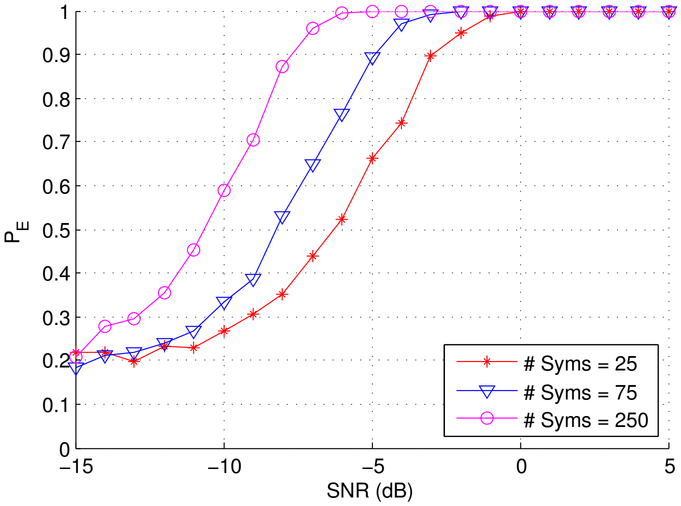


Figure 3.11: Probability of correct estimation of CP length N_g.

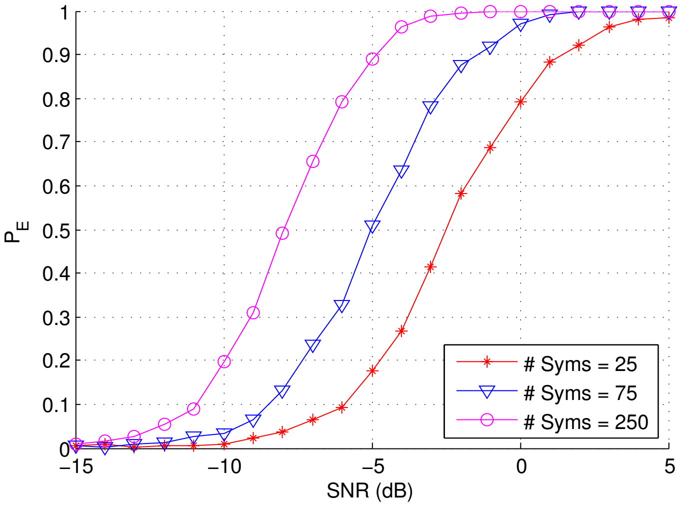


Figure 3.12: Probability of correct estimation of delay θ.

To determine the impact of the CP order Figure 3.13, Figure 3.14 and Figure 3.15 present the performance of the synchronization parameter estimators with a 75 symbol DL sub frame length and possible CP lengths. All assumptions and other signal properties are the same as the signal described in the previous paragraph. It can be observed from the

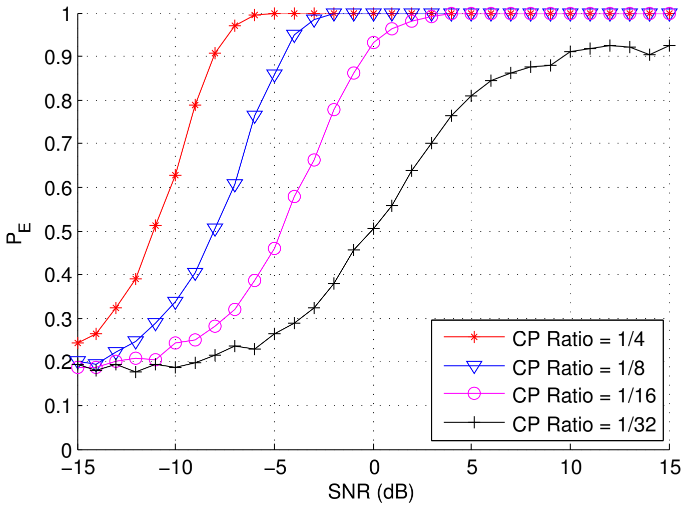


Figure 3.13: Probability of correct estimation of symbol length N_b for varying CP lengths and 75 symbol frame length.

figures that the performance of the estimator decreases as the CP length decreases. This is expected as the estimator exploits the cyclostationary properties of the CP to perform correct estimation.

It can be noted that from Figure 3.13, Figure 3.14 and Figure 3.15 for the CP ratio of $\frac{1}{32}$ the estimator is unable to achieve an estimation probability of one for all synchronization parameters. In this case estimation is limited by the number of symbols available to the estimator. Figure 3.16 demonstrates that with when a greater number of symbols are available the synchronization parameters can be estimated where 250 symbols per frame are received, rather then 75, for CP length $\frac{1}{32}$ while all other signal parameters remain the same as the first paragraph in this sub section.

3.3.5 CFO Estimation.

The CFO estimator is developed as the theory presented in Section 2.3.6. Figure 3.17 presents the performance of the CFO estimator. The simulation uses a received base band

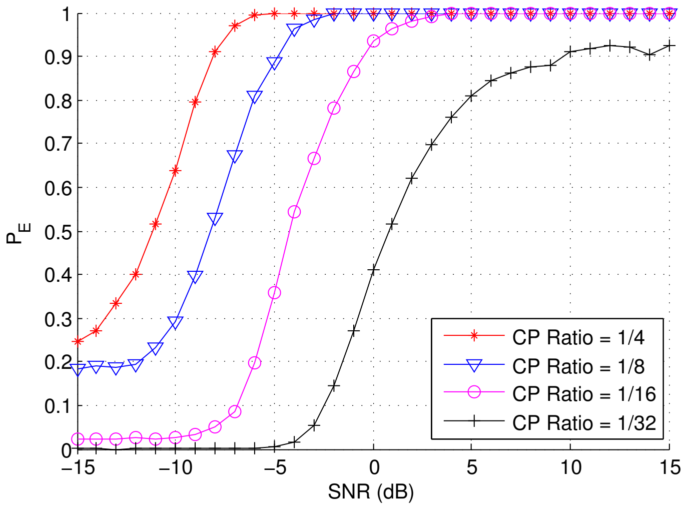


Figure 3.14: Probability of correct estimation of CP length N_g for varying CP lengths and 75 symbol frame length.

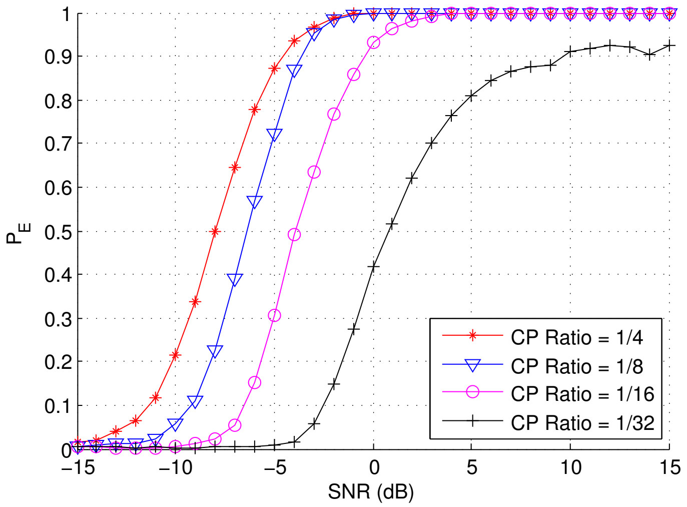


Figure 3.15: Probability of correct estimation of delay θ for varying CP lengths and 75 symbol frame length.

down sampled and pulse shaped removed signal for varying frame lengths in symbols. The signal is generated with a CFO of $\epsilon = 0.25$ and CP ratio of $\frac{1}{4}$.

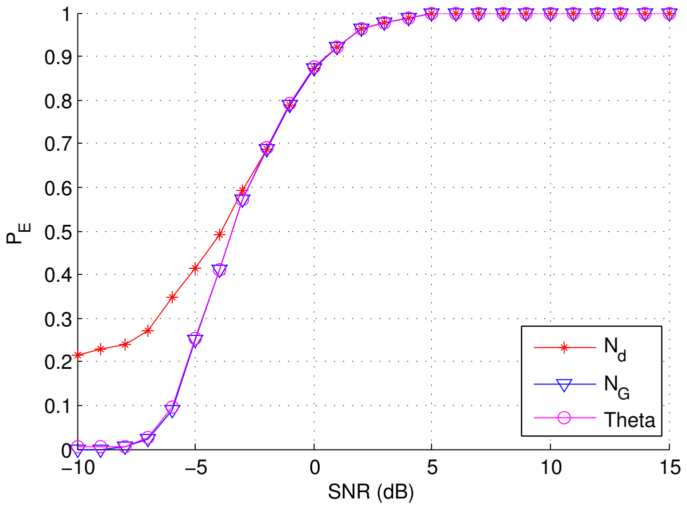


Figure 3.16: Probability of correct estimation of synchronization parameters for CP length $\frac{1}{32}$ and 250 symbol frame length.

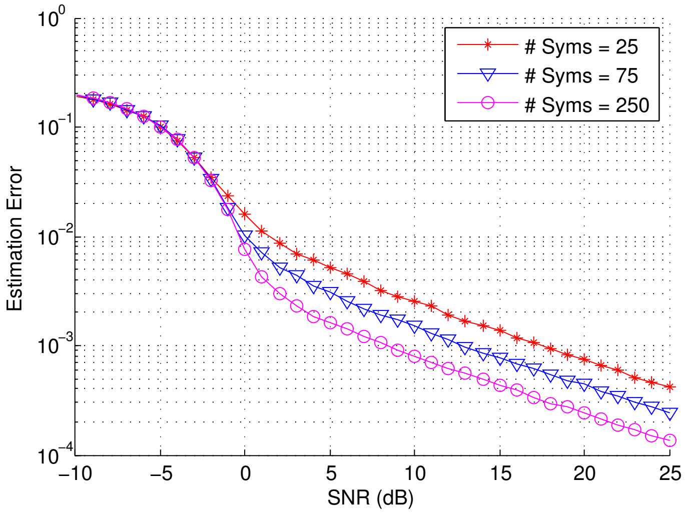


Figure 3.17: Mean absolute estimation error of CFO ϵ.

To determine the impact of the CFO magnitude Figure 3.18 presents the performance for a fixed SNR of 8 dB for varying CFO. The CFO ϵ is bound between 0 and 0.45 of the SC spacing as the estimator is not valid for CFO of $|\epsilon| \geq 0.5$. All assumptions and

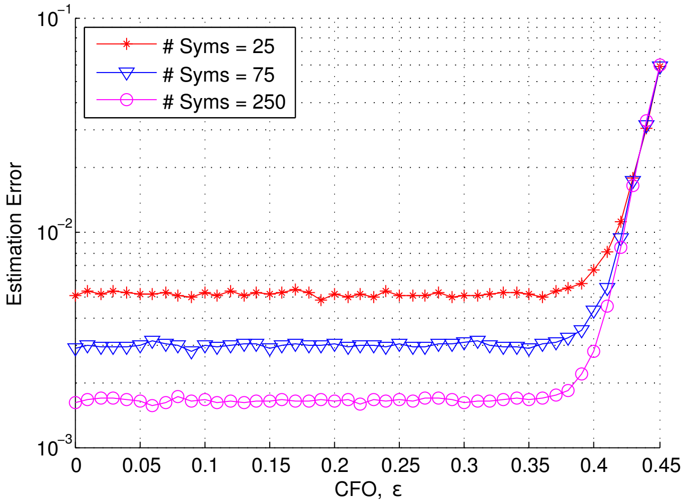


Figure 3.18: Mean absolute estimation error of CFO ϵ for varying ϵ.

other signal properties are the same as the signal described in the previous paragraph. In Figure 3.18 it can be observed that the performance of the CFO estimator does not vary until the magnitude of the CFO approaches $\epsilon = 0.5$ where the estimator is not valid.

To determine the impact of CP length on CFO estimation Figure 3.19 presents the estimator's performance for a 75 symbol frame length and varying CP length. All assumptions and other signal properties are the same as the signal described in the first paragraph of this sub section. It can be observed that as the CP decreases the estimation error increases as the CFO estimator has less CP samples available.

3.4 Jamming BDA Model

Figure 3.20 presents the model which performs jamming BDA by observing LA of SCs between subsequent OFDMA frames. The model is based on the theory presented in Section 2.4. If the burst profile is available the model presented performs BDA using the modulation signaling, otherwise modulation type must be classified as exhibited by the red dashed decision path. Note that both cases result in the same end state which is

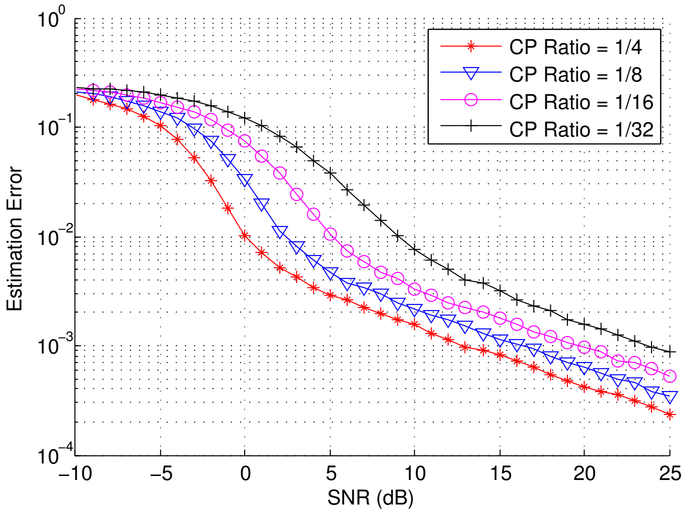
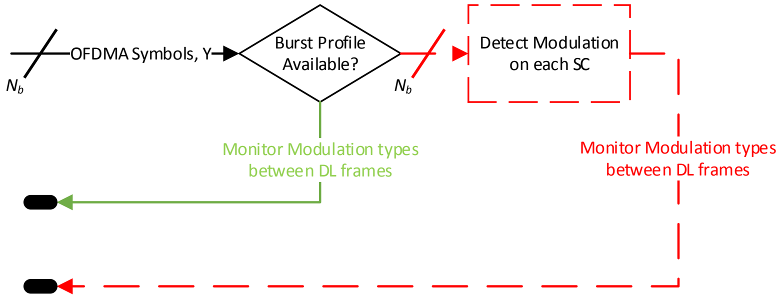


Figure 3.19: Mean absolute estimation error of CFO ϵ for varying CP and 75 symbol frame length.



N_b
OFDMA Symbols, Y
Burst Profile Available?
N_b
Detect Modulation on each SC
Monitor Modulation types between DL frames
Monitor Modulation types between DL frames

Figure 3.20: Jamming BDA model.

observing modulation change between OFDMA DL sub frames. The model operates on each OFDMA DL sub frame, of varying lengths in symbols, as SC modulation remains constant within each sub frame as detailed in Section 2.2.2.

In the case where a burst profile is unavailable the performance of the modulation classifier is investigated in the following paragraphs. The classification probability for different modulation types is considered as it will vary as the size of the ML classifier

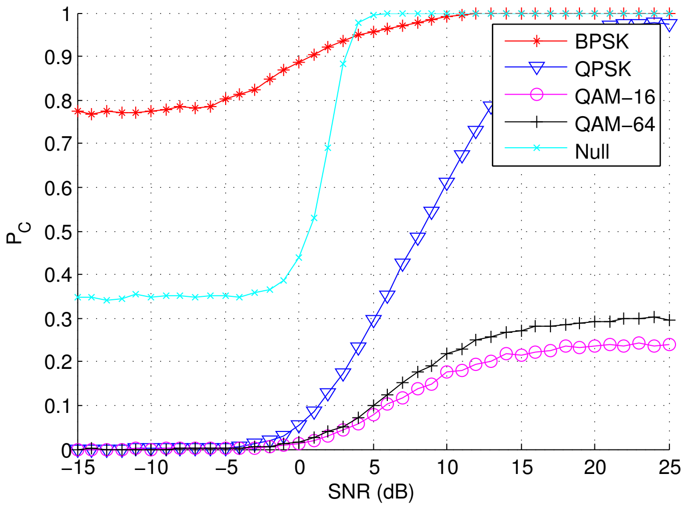


Figure 3.21: Probability of correct modulation classification with a 25 symbol frame length.

decision regions are not the same and CFO impact the classification of modulation types differently. Figure 3.21, Figure 3.22 and Figure 3.23 present the classification performance of SCs for all possible modulation types for frame lengths of 25, 75 and 250 symbols respectively. The simulations are performed for a received base band, down sampled, matched filtered, CP removed signal, with no CFO for varying frame lengths in symbols.

From Figure 3.21, Figure 3.22 and Figure 3.23 it can be observed that the greater the number of symbols per frame the better the probability of SC classification. This is expected as the cumulant sample estimates variance reduces when a greater number of samples are available. In addition, the SC modulation classifier is not adept at classifying QAM modulation types even at high SNRs and number of symbols per frame. Table 3.1 presents the confusion matrix for the SC estimation at a SNR of 20 dB and 250 symbols. From the confusion matrix it is apparent that the classifier has difficulty classifying QAM modulation types, yet, it does distinguish between PSK and QAM modulation. QAM

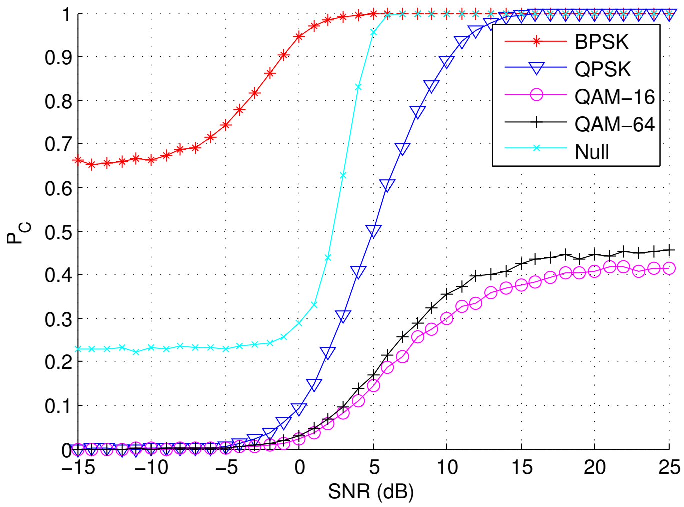


Figure 3.22: Probability of correct modulation classification with a 75 symbol frame length.

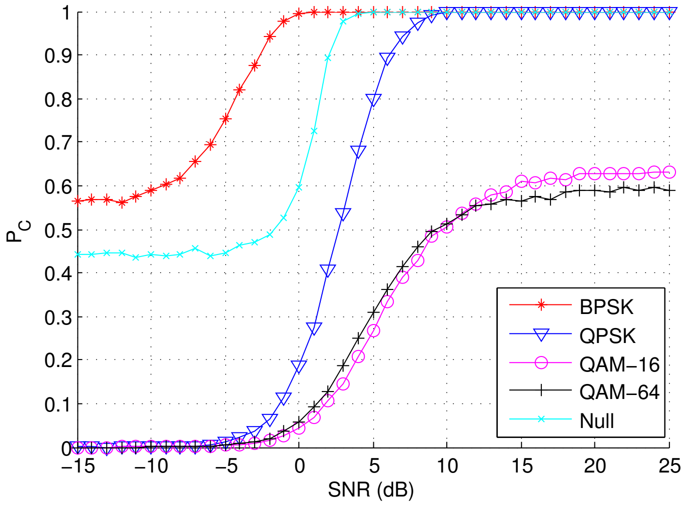


Figure 3.23: Probability of correct modulation classification with a 250 symbol frame length.

modulation types are difficult to classify as their cumulant statistics are similar. To overcome the difficulty classifying QAM modulation types a large numbers of samples are required. As this work only considers 25, 75, and 250 symbols per frame, and typically

Table 3.1: Confusion Matrix for SC classification at SNR = 20 dB, 6000 trials and a 250 symbol frame length.

		True				
		BPSK	QPSK	QAM-16	QAM-64	Null
Classified (%)	BPSK	6000 (100)	0 (0)	0 (0)	0 (0)	0 (0)
	QPSK	0 (0)	6000 (100)	546 (9)	169 (3)	0 (0)
	QAM-16	0 (0)	0 (0)	3585 (60)	2408 (40)	0 (0)
	QAM-64	0 (0)	0 (0)	1869 (31)	3413 (57)	0 (0)
	Null	0 (0)	0 (0)	0 (0)	10 (0)	6000 (100)

an OFDMA frame may not consist of the number of symbols required, the variability when classify QAM modulation can be improved by grouping QAM modulation types. BDA can then be performed via observation of LA between the modulation types BPSK, QPSK, and grouped QAM. The performance increase of the classifier when QAM modulation is grouped is presented in Figure 3.24.

The impact of the preamble and pilot SCs on modulation classification must be considered. The preamble is the first OFDMA symbol of each DL sub frame where SCs are modulated utilizing boosted BPSK. For the considered DL sub frame lengths the preamble does not impact the statistics of the cumulant and consequently there is no observable difference of SC modulation classification without the preamble. As detailed in Section 2.2.1 pilot SCs are modulated as boosted BPSK on alternating SCs for odd and even symbols. As the pilot SCs alternate, data is also modulated onto the same SCs every second symbol. The probability of the pilot SCs being classified as BPSK is detailed in Figure 3.25 for each possible modulation on the pilot SCs. Null is not considered as it is not used to modulate data SCs. A signal with 250 symbols is used and other parameters are the same

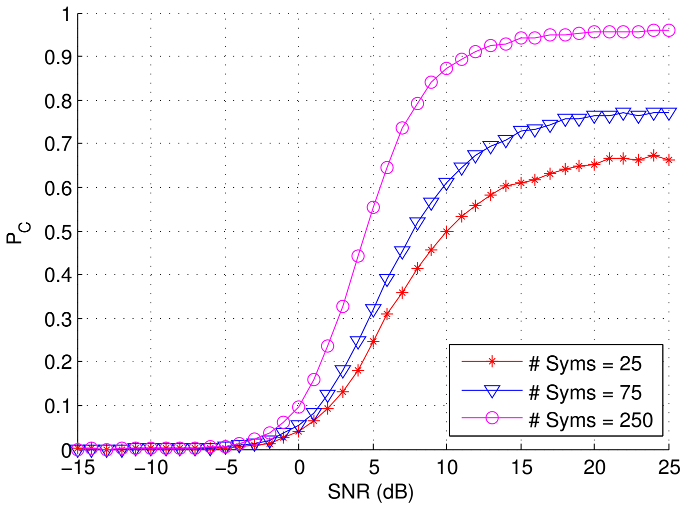


Figure 3.24: Probability of correct modulation classification of QAM modulation when QAM-16/64 are grouped.

as the signal in the first simulation in this section. It can be observed that the alternating data modulation used on the pilot SCs does not significantly impact the probability that pilot SCs are classified as BPSK.

The impact of CFO on the SC modulation classifier's performance is presented in Figure 3.26 where a CFO of $\epsilon = 0.25$ is simulated for a frame length of 250 symbols and all other parameters are the same as the first simulation in this section. By comparing Figure 3.23 and Figure 3.26 it can be noted that CFO significantly degrades the classification performance of all modulation types. Table 3.2 presents the confusion matrix for SC estimation at a SNR of 20 dB and 250 symbols. From the confusion matrix it is apparent that the estimator can not distinguish between modulation types in the presence of CFO. Further, a trend exists where modulation types are classified as types with smaller cumulants. This is expected as the CFO tends to cause the modulation constellations to appear increasingly random, causing their respective cumulants to approach zero. As the cumulant approaches zero the modulation type is classified as null.

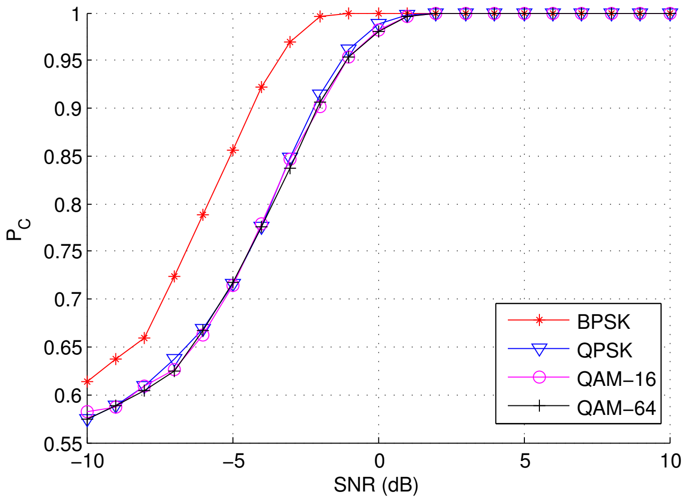


Figure 3.25: Probability of correct modulation classification of pilot SC as BPSK for possible modulation types with a 250 symbol frame length.

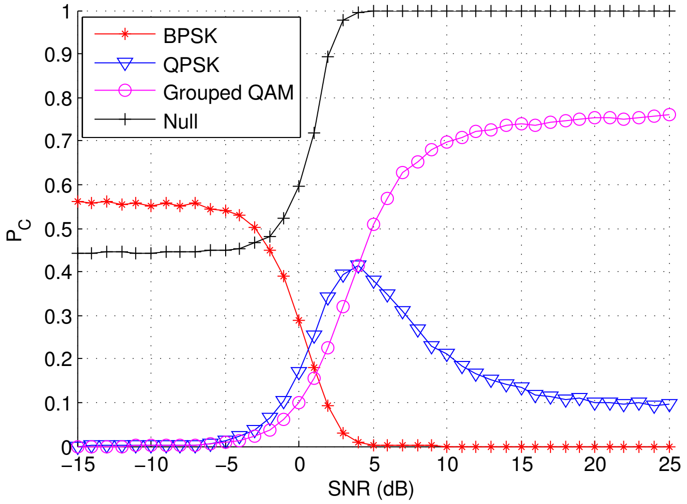


Figure 3.26: Probability of correct modulation classification with CFO $\epsilon = 0.25$ and a 250 symbol frame length.

Figure 3.27 presents the SC modulation classifier's performance when the CFO estimator is employed to correct the CFO. Note, that the CFO estimator performance

Table 3.2: Confusion Matrix for SC classification at SNR = 20 dB, 6000 trials with CFO and a 250 symbol frame length.

		True			
		BPSK	QPSK	Grouped QAM	Null
Classified (%)	BPSK	0 (0)	0 (0)	0 (0)	0 (0)
	QPSK	0 (0)	591 (10)	3 (0)	0 (0)
	Grouped QAM	911 (15)	5409 (90)	4524 (75)	0 (0)
	Null	5089 (85)	0 (0)	1473 (25)	6000 (100)

increases with SNR. All other signal properties are the same as the simulation in the previous paragraph. Comparing Figure 3.26 and Figure 3.27 it can be concluded that the CFO estimator increases classification performance as SNR increases. This occurs as at high SNRs the CFO can be successfully estimated with small error and corrected before SC classification.

The minimum CFO estimation error required for modulation classification can be determined by considering Figure 3.27. An acceptable probability of classification of BPSK modulation is 75% which occurs at a SNR of approximately 10 dB when the signal has a 250 symbol frame length. By referring to the CFO estimator performance in Figure 3.17 the estimation error is approximately $|\epsilon| < 0.001$ at an SNR of 10 dB. This value of CFO is then determined as a threshold for successful CFO estimation and is employed in Chapter IV.

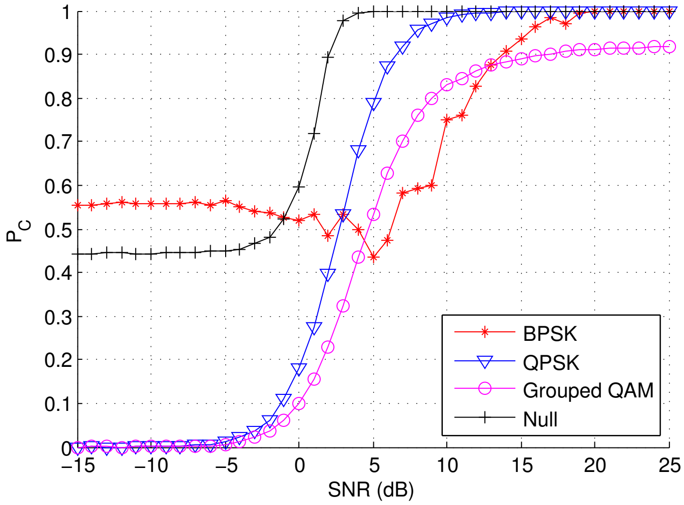


Figure 3.27: Probability of correct modulation classification with corrected CFO and a 250 symbol frame length.

IV. Results

This chapter evaluates the overall performance of the OFDMA blind demodulation model and jamming BDA model in a perfect channel and multi-path channel. Firstly, all the parameters of a pass band OFDMA signal are estimated, and performance is presented, and used for demodulation. The blindly demodulated signal is then used to evaluate the performance of the SC modulation classifier.

4.1 Blind Demodulation and Jamming BDA Performance in a Perfect Channel

This section evaluates the performance of the OFDMA blind demodulation and jamming BDA model in a perfect channel.

4.1.1 OFDMA Blind Demodulation Model Performance.

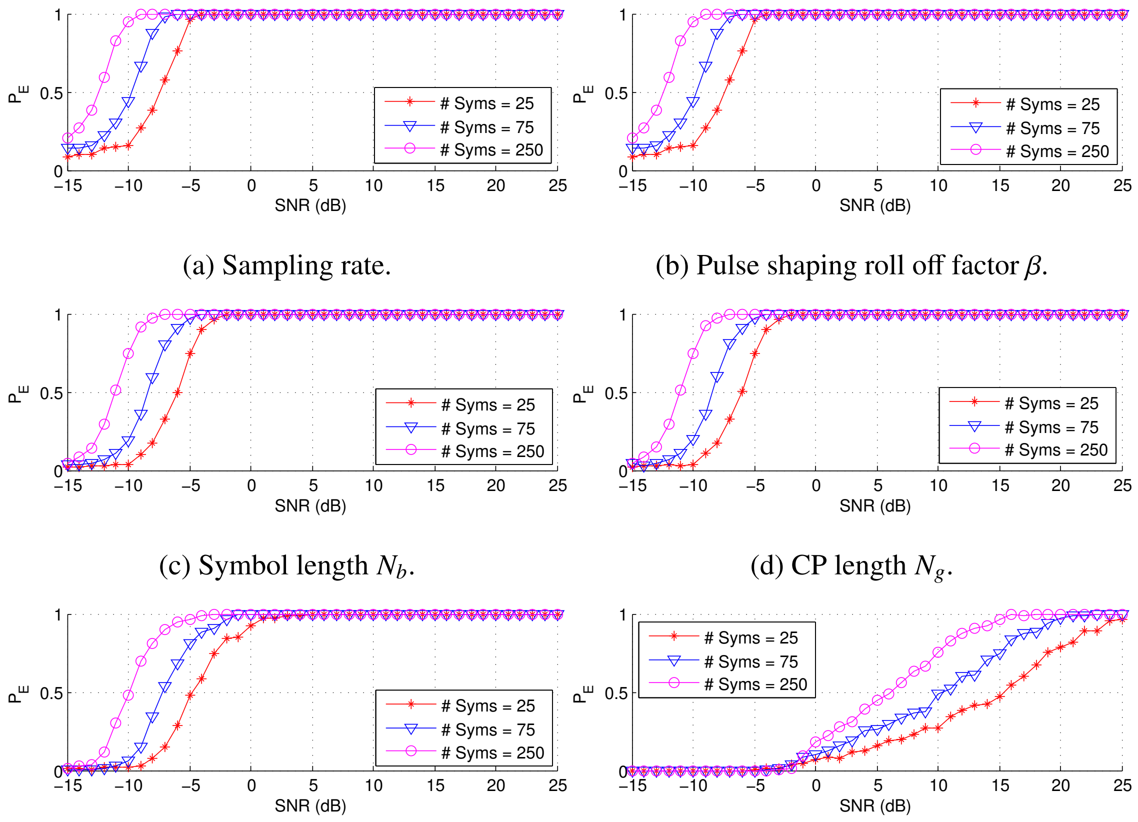
To evaluate the performance of the OFDMA blind demodulation model simulations are performed utilizing an OFDMA signal with a 10 kHz carrier frequency, 5 kHz BW, up sampling rate of 8, oversampling rate of 1, pulse shaping roll off factor of 0.7, and CP ratio of $\frac{1}{4}$. Varying modulation types are not considered as they do not impact blind demodulation. The impact of SC modulation, however, is considered when evaluating the performance of the BDA model. For blind demodulation, probability of estimation is considered rather then absolute estimation error for the roll off factor and CFO estimators. This is performed as it illustrates what SNRs the absolute estimation error is small enough to enable subsequent parameter estimation. The threshold for the roll off factor estimation is an absolute error less than 0.05. The CFO ϵ is determined to be successfully estimated when the absolute estimation error is less than 0.001. This value of the CFO enables, at a sufficient SNR, a 75% classification of BPSK modulation for a 250 symbol frame length and is derived in Section 3.4. For the simulations a carrier frequency is used to down mix the signal with a CFO fixed at $\epsilon = 0.25$, while the delay θ is drawn from a uniform distribution on the interval $\{\theta | 0 \leq \theta < N_b\}$. The CFO is fixed as the performance of the CFO estimator does not vary until ϵ approaches 0.5.

Following removal of the carrier frequency the sampling rate and the roll off factor are estimated and performance is presented in Figure 4.1 (a) and (b) respectively. With the estimated sampling rate and roll off factor the signal is matched filtered, and down sampled. Figure 4.1 (c), (d) and (e) present the performance of the symbol length N_b, CP length N_g and delay θ estimators respectively. Utilizing the estimated synchronization parameters the OFDMA signal is synchronized. Figure 4.1 (f) presents the performance of the CFO estimator. From the presented figures it can be concluded that the blind demodulator's performance is limited by CFO estimation while increased number of symbols improves performance.

4.1.2 Jamming BDA Model Performance.

The blindly demodulated signal is used to evaluate the performance of the BDA model. In the scenario where the burst profile is available the signaling information is used to determine modulation type. In this instance the BDA model would share performance with the blind demodulation model. In the case that the burst profile is unavailable the modulation is determined utilizing the modulation classifier.

Figure 4.2, Figure 4.3 and Figure 4.4 present the performance of the modulation classifier for 25, 75 and 250 symbol frame lengths respectively. Note that at low SNRs for all modulation types the probability of classification is zero. This occurs as the signal could not be blindly demodulated and consequently no SCs could be classified. Table 4.1 presents the confusion matrix for SC classification at a SNR of 20 dB and 250 symbols. From the table it is apparent at a high SNR the model is adept at classifying between the four modulation types. It is expected that the confusion with classifying the QAM modulation types would decrease with increased number of symbols per frame as the cumulant sample estimates would have reduced variance. Further, comparing the



(a) Sampling rate.

(b) Pulse shaping roll off factor β.

(c) Symbol length N_b.

(d) CP length N_g.

(e) Delay θ.

(f) CFO ϵ.

Figure 4.1: Probability of correct estimation of the blind demodulation parameters in a perfect channel.

classification probabilities presented in Figure 3.27 and Figure 4.4 it can be observed that the performance of the classifier is being limited by that of the CFO estimator, as explored in Section 3.4. At low SNRs it also appears that the SC classifier's performance is limited by the blind demodulator, however, if the signal could be blindly demodulated at such SNRs the classifier could not discern between modulation types.

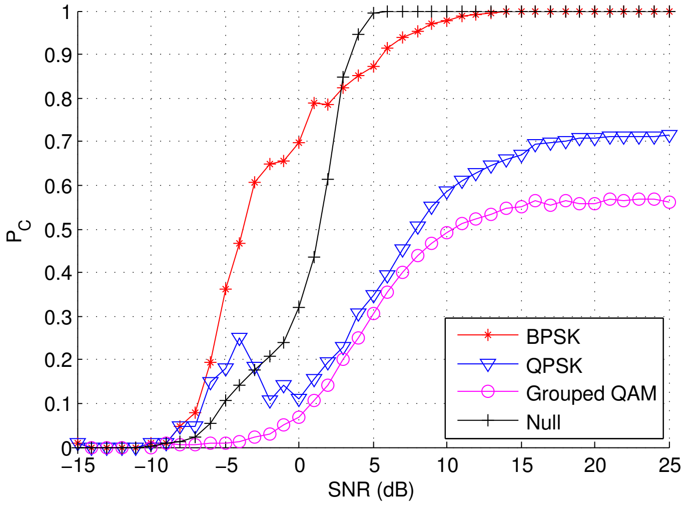


Figure 4.2: Probability of correct modulation classification with a 25 symbol frame length in a perfect channel.

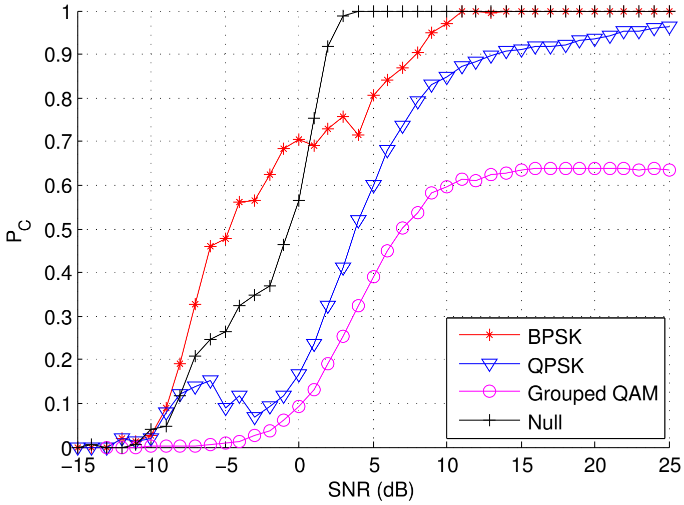


Figure 4.3: Probability of correct modulation classification with a 75 symbol frame length in a perfect channel.

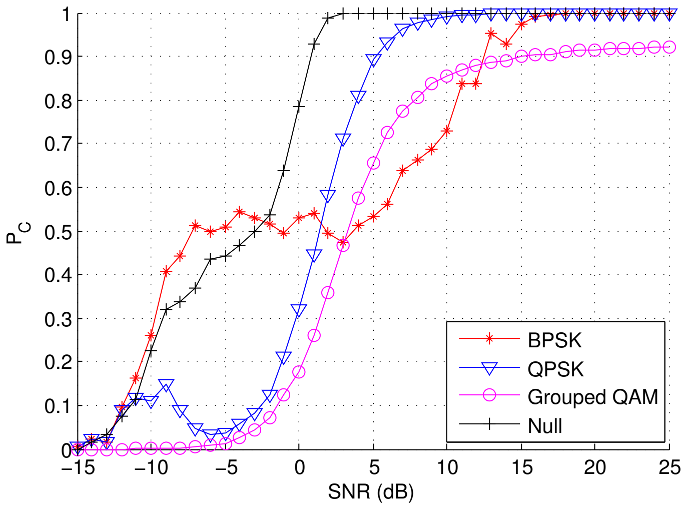


Figure 4.4: Probability of correct modulation classification with a 250 symbol frame length in a perfect channel.

Table 4.1: Confusion Matrix for SC classification at SNR = 20 dB, 6000 trials and 250 symbols in a perfect channel.

		True			
		BPSK	QPSK	Grouped QAM	Null
Classified (%)	BPSK	6000 (100)	0 (0)	0 (0)	0 (0)
	QPSK	0 (0)	6000 (100)	509 (8)	0 (0)
	Grouped QAM	0 (0)	0 (0)	5490 (92)	0 (0)
	Null	0 (0)	0 (0)	1 (0)	6000 (100)

4.2 Blind Demodulation and Jamming BDA Performance in a Multi-path Channel

This section evaluates the performance of the OFDMA blind demodulation and jamming BDA model in a single multi-path channel.

4.2.1 OFDMA Blind Demodulation Model Performance.

To evaluate the performance of the OFDMA blind demodulation model simulations are performed utilizing the signal properties used in Section 4.1.1, however, a single multi-path channel is employed as detailed in Section 3.2.

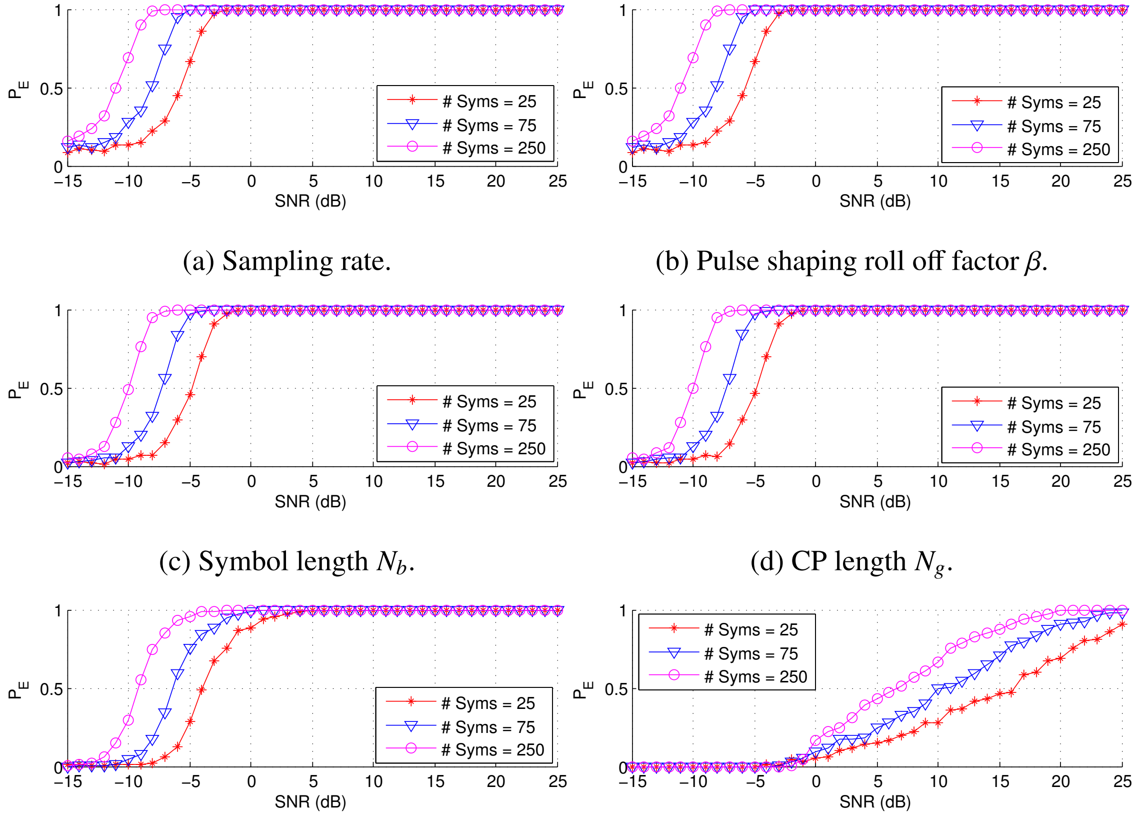
Following removal of the carrier frequency the sampling rate and the roll off factor are estimated and performance is presented in Figure 4.5 (a) and (b) respectively. Figure 4.5 (c), (d), and (e) present the performance of the synchronization parameter estimators. Figure 4.5 (f) presents the performance of the CFO estimator. The threshold which determines successful estimation for each parameter is introduced in Section 4.1.1.

By comparing Figure 4.1 and Figure 4.5 it can be concluded that the blind demodulator performance is degraded in the single multi-path channel by approximately 2 dB for all but the CFO estimator. The CFO estimator performance is degraded by approximately 5 dB. It would be expected that performance would degrade further with more complex multi-path channels where higher SNRs would be required to perform blind demodulation. The blind demodulator would be expected to operate in multi-path channel unless the channel varies faster then the OFDMA symbol rate. In this case blind demodulation may fail as the repetition of the CP can no longer be exploited to determine the synchronization parameters. The impact of more complex channels require exploration in future work.

4.2.2 Jamming BDA Model Performance.

The jamming BDA model is evaluated utilizing the blindly demodulated signal. In the case that the burst profile is available it is assumed equalization can be performed due to known signal equalization parameters such as pilots or preamble which are available once the signal is demodulated.

Figure 4.6 presents the performance of the modulation classifier for a 250 symbol frame length. From the figure it is apparent that the single multi-path channel significantly impacts the modulation classifier's performance. Table 4.2 presents the confusion matrix



(a) Sampling rate.

(b) Pulse shaping roll off factor β.

(c) Symbol length N_b.

(d) CP length N_g.

(e) Delay θ.

(f) CFO ϵ.

Figure 4.5: Probability of correct estimation of the blind demodulation parameters in a multi-path channel.

for SC classification at a SNR of 20 dB and 250 symbol frame length. The confusion matrix exhibits that there is increased classifier confusion, when compared to the perfect channel, between all modulation types at the same SNRs. The degradation of performance is expected as the classifier is not robust in a multi-path environment and increased degradation would occur in more complex channels. To overcome the performance degradation due to the multi-path channel a method of blind channel equalization is required. Blind equalization is recommended as future work.

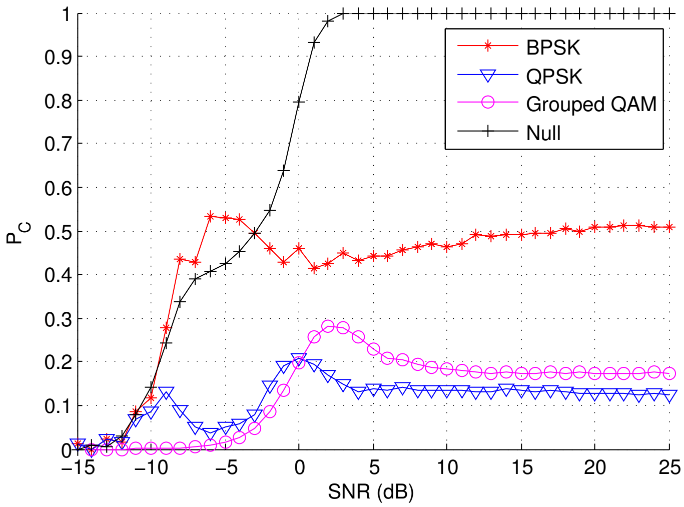


Figure 4.6: Probability of correct modulation classification with a 250 symbol frame length in a multi-path channel.

Table 4.2: Confusion Matrix for SC classification at SNR = 20 dB, 6000 trials and 250 symbols in a multi-path channel.

		True			
		BPSK	QPSK	Grouped QAM	Null
Classified (%)	BPSK	3043 (50)	2141 (35)	227 (4)	0 (0)
	QPSK	1059 (18)	769 (13)	1949 (33)	0 (0)
	Grouped QAM	1882 (31)	1492 (25)	1035 (17)	0 (0)
	Null	16 (1)	1598 (27)	2789 (46)	6000 (100)

V. Summary

5.1 Conclusion

It is a key objective of the United States Military, and coalition partners, to control the RF spectrum. An aspect of the control of the RF spectrum is developing techniques to affect emerging wireless broadband communication technologies such as OFDMA. Consequently, this research presents a new method to blindly demodulate a pass band OFDMA signal by extending, modifying, and collating previous research and introduces a novel technique to perform jamming BDA, on the demodulated signal, via observing modulation LA. To perform these tasks, following signal generation, two models are introduced which are a blind demodulation and jamming BDA model. The performance of these models is assessed by varying multiple parameters at different noise levels. The general trend of performance for the blind demodulation model and BDA model is that parameter estimation is limited by CFO estimation, CP length and the number of OFDMA symbols per DL sub frame. It is concluded that the BDA model performance can be improved if QAM modulation types are grouped as for a small number of symbols there is insufficient statistics to distinguish between QAM modulation types. LA can then be observed between BPSK, QPSK and QAM modulation types. It was demonstrated that at a SNR of 20dB and 250 symbols per OFDMA DL sub frame the SC modulation types BPSK, QPSK and null could be correctly classified for all trials, while grouped QPSK was classified for greater than 90% of trials. Further, pilot SCs tended to be estimated as BPSK modulation regardless of the other alternative data modulation type. The performance of both models is also assessed in a single multi-path environment. The blind demodulation model is adept in the single multi-path environment, while, SC modulation classification experienced significantly degraded performance. Fortunately, the method to estimate SC modulation may be extended to also perform blind equalization using methods akin to that detailed in [34] which would improve classification performance.

5.2 Future Work

It is shown that the introduced method for blind demodulation is effective in a single multi-path channel, however, SC classification for BDA experienced decreased performance. To successfully achieve SC classification in a multi-path channel requires blind channel equalization. Fortunately, cumulant based SC classification and blind channel equalization methods have been proposed in the literature such as [34]. Alternatively, other modulation type classification techniques could be employed which may be effective in the multi-path environment such as more complex decision theoretic approaches. Following development of a method of SC classification in a multi-path channel more complex multi-path environments should be considered.

To perform blind demodulation this research assumes that only the OFDMA signal exists in the communication channel. This is not practical in a real channel and consequently work exists in the detection and frequency windowing of the OFDMA signal in a channel with various communication systems. Further, the carrier frequency is assumed to be estimated with a maximum CFO of half the SC spacing. Blind estimation of the carrier frequency could be considered as future work.

There is significant computational complexity required to estimate the pulse shaping filter roll off factor and sampling rate. Work could be performed to reduce the complexity of these detectors. In addition the sampling rate estimator is biased and could be adapted to an unbiased estimator as detailed in [11].

There is also exploration left in the parameters that determine the performance of the blind demodulation and BDA models. For the simulations performed it is assumed there is no STO, however with the proposed method a STO may exist. This issue could be fixed by modifying the estimation method, or the effects of STO on demodulation could simply be explored. Different FFT sizes can also be considered.

Work could also be extended to exploit the blind demodulation and classification of SC to intercept adversary's data or perform advanced jamming techniques such as pilot or CP jamming.

Bibliography

[1] "IEEE Standard for Local and metropolitan area networks," *IEEE Std 802.16*, 2009.

[2] A. Swami and B. Sadler, "Hierarchical digital modulation classification using cumulants," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 416–429, 2000.

[3] R. Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, Inc., Norwood, MA, USA, 1st edition, 2000.

[4] W. Hoeg and T. Lauterbach, *Digital audio broadcasting: principles and applications of digital radio*, Wiley, 2003.

[5] M. Ergen, *Mobile Broadband: Including WiMAX and LTE*, Information Technology: Transmission, Processing and Storage. Springer, 2009.

[6] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communications with MATLAB*, Wiley, 2010.

[7] L. Nir, T. Waterschoot, M. Moonen, and J. Duplicy, "Blind CP-OFDM and ZP-OFDM Parameter Estimation in Frequency Selective Channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 11:1–11:10, Jan. 2009.

[8] Y. Chan, J. Plews, and K. Ho, "Symbol rate estimation by the wavelet transform," in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS)*, 1997, vol. 1, pp. 177–180.

[9] M. Flohberger, W. Kogler, W. Gappmair, and O. Koudelka, "Symbol rate estimation with inverse fourier transforms," in *International Workshop on Satellite and Space Communications*, 2006, pp. 110–113.

[10] Z. Yu, Y. Shi, and W. Su, "Symbol-rate estimation based on filter bank," in *Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS)*, 2005, vol. 2, pp. 1437–1440.

[11] L. Mazet and P. Loubaton, "Cyclic correlation based symbol rate estimation," in *Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers*, 1999, vol. 2, pp. 1008–1012.

[12] W. Gardner, "Exploitation of spectral redundancy in cyclostationary signals," *IEEE Signal Processing Magazine*, vol. 8, no. 2, pp. 14–36, 1991.

[13] M. Shi, Y. Bar-Ness, and W. Su, "Blind OFDM Systems Parameters Estimation for Software Defined Radio," in *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2007, pp. 119–122.

[14] H. Xu, Y. Zhou, and Z. Huang, “Blind Roll-Off Factor and Symbol Rate Estimation Using IFFT and Least Squares Estimator,” in *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, 2007, pp. 1052–1055.

[15] E. Terzi, *Blind synchronization and detection of Nyquist pulse shaped QAM signals*, Masters thesis, University of South Florida, 2009.

[16] M. Shi, *Advanced classification of OFDM and MIMO signals with enhanced second order cyclostationarity detection*, Ph.D. thesis, New Jersey Institute of Technology, 2010.

[17] H. Ishii and G. Wornell, “OFDM Blind Parameter Identification in Cognitive Radios,” in *IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2005, vol. 1, pp. 700–705.

[18] P. Liu, B. Li, Z. Lu, and F. Gong, “A blind time-parameters estimation scheme for OFDM in multi-path channel,” in *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, 2005, vol. 1, pp. 242–247.

[19] T. Yucek and H. Arslan, “OFDM Signal Identification and Transmission Parameter Estimation for Cognitive Radio Applications,” in *IEEE Global Telecommunications Conference (GlobeCom)*, 2007, pp. 4056–4060.

[20] H. Nogami, S. Tsuruga, and N. Morinaga, “A transmission mode detector for OFDM systems,” *Electronics and Communications in Japan (Part I: Communications)*, vol. 86, no. 8, pp. 79–94, 2003.

[21] J. van de Beek, M. Sandell, and P. Borjesson, “ML estimation of time and frequency offset in OFDM systems,” *IEEE Transactions on Signal Processing*, vol. 45, no. 7, pp. 1800–1805, 1997.

[22] P. Moose, “A technique for OFDM frequency offset correction,” *IEEE Transactions on Communications*, vol. 42, no. 10, pp. 2908–2914, 1994.

[23] T. Schmidl and D. Cox, “Robust frequency and timing synchronization for OFDM,” *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, 1997.

[24] F. Gini and G. Giannakis, “Frequency offset and symbol timing recovery in flat-fading channels: a cyclostationary approach,” *IEEE Transactions on Communications*, vol. 46, no. 3, pp. 400–411, 1998.

[25] K. Jayanthi, *Some investigations on quality improvement using link adaptation techniques in cellular mobile networks*, Ph.D. thesis, Pondicherry University, 2006.

[26] T. Yucek and H. Arslan, "A novel sub-optimum maximum-likelihood modulation classification algorithm for adaptive OFDM systems," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2004, vol. 2, pp. 739–744.

[27] S. Reddy, T. Yucek, and H. Arslan, "An efficient blind modulation detection for adaptive OFDM systems," in *Vehicular Technology Conference*, 2003, vol. 3, pp. 1895–1899.

[28] T. Keller and L. Hanzo, "Blind-detection assisted sub-band adaptive turbo-coded OFDM schemes," in *Vehicular Technology Conference*, 1999, vol. 1, pp. 489–493.

[29] X. Huo and D. Donoho, "A simple and robust modulation classification method via counting," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, 1998, vol. 6, pp. 3289–3292.

[30] B. Mobasseri, "Constellation shape as a robust signature for digital modulation recognition," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, 1999, vol. 1, pp. 442–446.

[31] P. Panagiotou, A. Anastasopoulos, and A. Polydoros, "Likelihood ratio tests for modulation classification," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, 2000, vol. 2, pp. 670–674.

[32] J. Sills, "Maximum-likelihood modulation classification for PSK/QAM," in *Proceedings of the IEEE Military Communications Conference (MILCOM)*, 1999, vol. 1, pp. 217–220.

[33] O. Dobre, A. Abdi, Y. Bar-Ness, and W. Su, "Survey of automatic modulation classification techniques: classical approaches and new trends," *Communications, IET*, vol. 1, no. 2, pp. 137–156, 2007.

[34] A. Swami, S. Barbarossa, and B. Sadler, "Blind source separation and signal classification," in *Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems, and Computers*, Oct 2000, vol. 2, pp. 1187–1191.

[35] R. Gray, *Identification and Classification of OFDMA Signals used in Next Generation Wireless Systems*, Masters thesis, Naval Postgraduate School, 2012.

[36] S. Tu, K. Chen, and R. Prasad, "Spectrum sensing of OFDMA systems for cognitive radios," in *IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2007, pp. 1–5.

[37] MATLAB, *version 8.2 (R2013b)*, The MathWorks Inc., Natick, Massachusetts, 2013.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704–0188*

1. REPORT DATE *(DD–MM–YYYY)* 27–03–2014	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From — To)* Oct 2012–Mar 2014

4. TITLE AND SUBTITLE Blind demodulation of pass band OFDMA signals and Jamming Battle Damage Assessment utilizing Link Adaptation	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Rutherford, Nicholas A., Flight Lieutenant, RAAF	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB, OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT-ENG-14-M-65
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) INTENTIONALLY LEFT BLANK	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

This research focuses on blind demodulation of a pass band OFDMA signal so that jamming effectiveness can be assessed; referred to in this research as BDA. The research extends, modifies and collates work within literature to perform a new method of blindly demodulating of a passband OFDMA signal, which exhibits properties of the 802.16 Wireless MAN OFDMA standard, and presents a novel method for performing BDA via observation of SC LA.
Blind demodulation is achieved by estimating the carrier frequency, sampling rate, pulse shaping filter roll off factor, synchronization parameters and CFO. The blind demodulator's performance in AWGN and a perfect channel is evaluated where it improves using a greater number OFDMA DL symbols and increased CP length. Performance in a channel with a single multi-path interferer is also evaluated where the blind demodulator's performance is degraded.
BDA is achieved via observing SC LA modulation behavior of the blindly demodulated signal between successive OFDMA DL sub frames in two scenarios. The first is where modulation signaling can be used to observe change of SC modulation. The second assumes modulation signaling is not available and the SC's modulation must be classified.
Classification of SC modulation is performed using sixth-order cumulants where performance increases with the number of OFDMA symbols. The SC modulation classifier is susceptible to the CFO caused by blind demodulation. In a perfect channel it is shown that SC modulation can be classified using a variety of OFDMA DL sub frame lengths in symbols. The SC modulation classifier experienced degraded performance in a multi-path channel and it is recommended that it is extended to perform channel equalization in future work.

15. SUBJECT TERMS

OFDMA, Battle Damage Assessment, Jamming, Blind Demodulation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Dr. Richard K. Martin (ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			
U	U	U	UU	85	**19b. TELEPHONE NUMBER** *(include area code)* (937) 255-3636 x4625 Richard.Martin@afit.edu